HACKER JOURNAL

Anno 2 - N. 19
13 Febbraio / 27 Febbraio 2003

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Contributors: Bismark.it, , Enzo Borri, CAT4R4TTA, Roberto "decOder" Enea, Loxeo, Paola Tigrino.

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Immagine di copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

SICUREZZA E INFORMAZIONI

Oggi sono stato ospite di una trasmissione della radio della Svizzera Italiana e che aveva per argomento la criminalità informatica.

Ho ovviamente iniziato chiarendo la distinzione tra hacker e cracker, tra appassionato e vandalo (o criminale). Ho potuto vedere che, in questo caso, spiegando chiaramente come stanno le cose, la differenza viene percepita.

Dove ho trovato qualche difficoltà, è stato nel chiarire l'importanza della libera circolazione delle informazioni riguardanti la sicurezza, informatica e non. Una simpatica signora che ha telefonato in studio, era piuttosto scandalizzata dal fatto che esistessero riviste come la nostra, che parlano senza peli sulla lingua di queste cose. Si chiedeva cosa accadrebbe se una rivista pubblicasse un tutorial su come sfruttare le debolezze di una cassaforte, dicendo che comunque è sbagliato farlo.

Cara signora ticinese: si sentirebbe davvero sicura se tenesse i suoi risparmi in una cassaforte che ha delle debolezze nascoste? Se la debolezza esiste, può star certa che gli addetti del settore (gli scassinatori) la conoscono: non vorrebbe saperne di più anche lei, in modo da poter prendere delle contromisure, oppure decidere di scegliere una cassaforte di marca diversa?

No cara signora: noi non abbiamo dubbi.

La vera sicurezza può derivare soltanto dalla massima conoscenza, e dalla massima circolazione delle informazioni.

Certo, se qualcuno scoprisse un problema nella sicurezza, dovrebbe prima di tutto avvertire il produttore, e concedergli un po' di tempo per prendere delle contromisure e avvisare i suoi clienti. Se questo però, come accade spesso nel mondo del software, fa orecchie da mercante, è più che giusto cercare di far circolare la notizia in altri modi.

grand@hackerjournal.it



Saremo di nuovo in edicola Giovedì 27 Febbraio!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

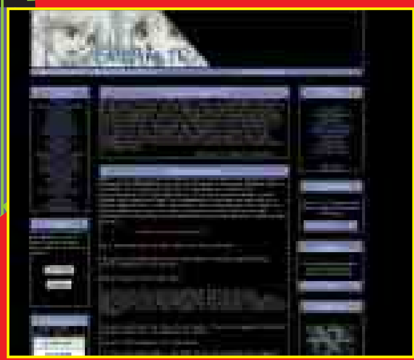
Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t



Dopo un periodo di inattività dovuto all'aggiornamento del server, è finalmente tornata attiva la possibilità di registrarsi un'email gratuita con indirizzo @hackerjournal.it La casella sarà accessibile attraverso l'interfaccia Web del sito, ma anche attraverso un normale client di posta POP3 (e questo, davvero, non è da tutti!). Per attivare la casella, basta entrare nella Secret Zone con le password che trovate in fondo a questa pagina. Una sola raccomandazione: trascrivete la password e non dimenticatela! Al momento infatti non è possibile recuperare una password persa, oppure modificarla.

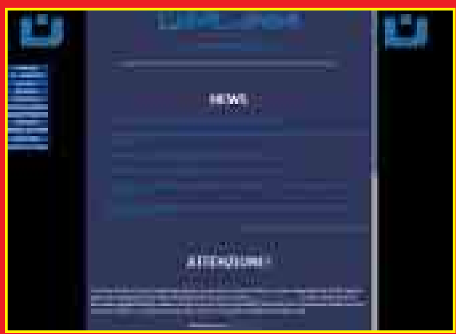




Dai bit alla carta

ECCO ALCUNI DEI VOSTRI SITI.
Se volete comparire in questo spazio, scrivete a: redazione@hackerjournal.it

www.divxdoor.too.it (DivX DooR)
www.uplink-italia.tk (SN4KE)
www.selphy.tk (witch_blade)
http://digilander.libero.it/andreaing (Andrea S.)
www.sistemavirale.cjb.net (Antonio)



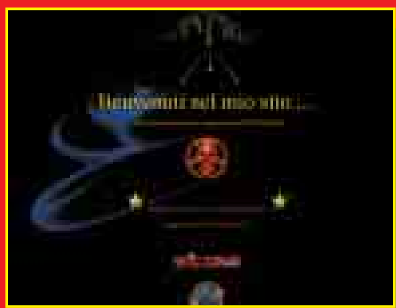


I MIGLIORI ARTICOLI

Il bello degli articoli del sito di HJ, è che li potete anche commentare. Potete scrivere il vostro parere, richiedere chiarimenti, fare correzioni o semplicemente ringraziare l'autore :-)
Ecco quindi la classifica di...

I 10 articoli più commentati

1. **Hacker, uno stile di vita** - (16 Commenti)
2. **CONNETTERSI CON LINUX by gaxt87** - (13 Commenti)
3. **Le basi del C** - (13 Commenti)
4. **Hacker's Prgramming Book** - (11 Commenti)
5. **Le basi del C parte quattro** - (10 Commenti)
6. **Open Source o Licenza d'uso?** - (9 Commenti)
7. **Kevin FREE!!!** - (9 Commenti)
8. **C#, un linguaggio tutto nuovo!** - (7 Commenti)
9. **Guida al C n. 5** - (7 Commenti)
10. **Il registro di sistema** - (6 Commenti)



Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: bassoven3
pass: inopport1

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

mailto:

redazione@hackerjournal.it

ATTACCANTE O ZOMBIE?

Mitica redazione di HJ ho un quesito da porvi: il Sygate m'ha rilevato per ben due volte un tentativo di scanning sul mio pc. Il 'Whois' m'ha portato in entrambe le occasioni ad una nota società e più precisamente all'IP di una persona con relativa sua e-mail. Gli ho scritto più volte e questo (molto infastidito) m'ha detto di smetterla xchè non sono il primo che lo accuso di un suo tentativo d'intrusione e, soprattutto, m'ha detto di lasciar perdere xchè non sono capace d'interpretare il Firewall!! Ora, cara redazione, mi spiegate che caxxo vuol dire 'Interpretare un Firewall'?!?! E soprattutto, che cosa dovrei fare se continuo ad avere segnalazioni dal Sygate? Grazie 1000 e continuate cosi'. (il mio indirizzo e-mail potete tranquillamente pubblicarlo).

Arj79

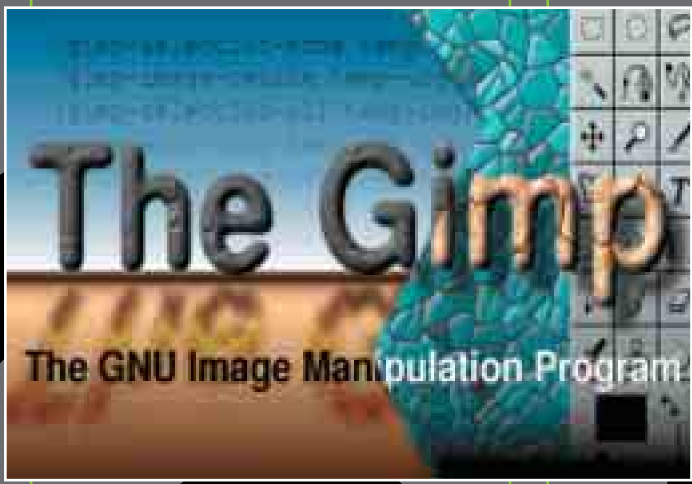
Mah, a occhio e croce direi che il tizio in questione viene usato, a sua insaputa, come testa di ponte da parte di qualcun altro. Probabilmente è stato trojanizzato, oppure utilizza un qualche tipo di proxy software (Wingate, per esempio), che fa ricadere su di lui le colpe delle incursioni di qualcun altro.

CI SIAMO CASCATI!



Non vi è passato per la testa che l'immagine della RIAA, pubblicata nella posta del numero 18, fosse fasulla?
Vi allego le immagini che ho trovato sul sito www.modernhumorist.com, sezione propaganda su internet. Guardate cosa c'è scritto in basso a sinistra…

Sigh… È vero. Ci siamo fidati troppo della segnalazione.



PROGRAMMI TROPPO COSTOSI

Carissima redazione di HJ,sono un ragazzo di Torino e vi scrivo perchè ho assolutamente bisogno del vostro aiuto;sono un appassionato di computer grafica,ma i programmi per mia o nostra sfortuna costano troppo. Conoscete per caso qualche sito dove scaricarli con tutorial compresi.

Grifis

Hai mai provato Gimp? È quasi potente come Photoshop, ma completamente grauito. Esiste per Linux, Mac (OS X con X11) e Windows. Lo trovi su http://www.gimp.org

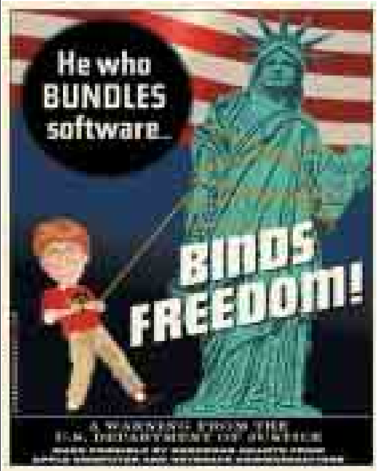
PROTEGGERE IL PC

Mi capita spesso di lasciare il mio PC in ufficio incustodito per recarmi in altre stanze. Poichè ho Win 98, come posso proteggere il PC dall'utilizo di malintenzionati? Oppure esiste un programma che mi permete di loggare le attività svolte sul mio PC in mia assenza?
Un'altra domanda, un tecnica.

Alessandro

Esistono dei programmi fatti apposta per questo scopo, che richiedono una password all'accensione, o che permettono di impostare un salvaschermo che può essere rimosso solo con una password (la funzione è presente anche nel salvaschermo di Windows, ma è ben poco sicura…). Trovi un bel po' di questi programmi su www.webattack.com/freeware/security/fwaccess.shtml Questi programmi fermano la maggior parte degli utenti, ma per i più smaliziati occorre qualche precauzione in più. Chiunque infatti potrebbe inserire un dischetto di sistema e riavviare il computer; in questo modo, anche se non potrebbe usare il tuo sistema, avrebbe accesso a tutti i tuoi file. Per evitarlo, devi entrare nel BIOS del tuo computer (premendo Canc all'avvio), ed effettuare alcune impostazioni. Innanzi tutto, nella parte "Boot se-



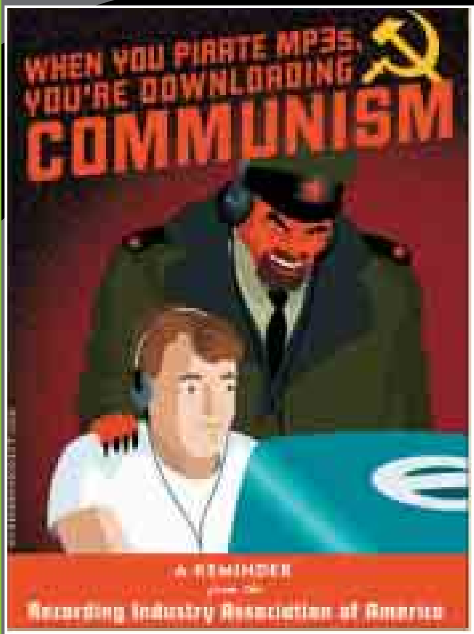


quence" devi abilitare solo il boot dall'hard disk principale, specificando anche di non cercare il sistema su altri supporti (floppy, CD-ROM). Poi, dovrai impostare una password per evitare che qualcuno modifichi le impostazioni del BIOS vanificando i tuoi sforzi. Cerca di segnarti la password e di non dimenticarla mai: potresti averne bisogno. Per esempi, se dovessi reinstallare il sistema operativo, avresti bisgono di riavviare da floppy o da CD, e senza password del BIOS non lo potresti fare.



ATTACCHI RIPETUTI E IP DINAMICI

Sulla mia makkina "Giulio" ho installato il firewall Zone Alarm un piccolo programma che mi ha fin da subito dato grandi soddisfazioni e mai nessun problema.
A ogni connessione che effettuo, noto che il firewall blocca sempre due o tre tentativi di connessione non autorizzata, sempre alle stesse porte e per di piu dallo stesso numero IP.



Avendo una connessione normale, e quindi un IP dinamico, la macchina che cerca di "spiarmi" come riesce ogni volta a rintracciarmi? In teoria ciò dovrebbe avvenire solo per una connessione e risolversi tutto alla mi disconnessione... Ma non è cosi

Grepz

Le possibilità sono tante... Innanzi tutto, se utilizzi Icq o un altro programma simile, il tuo attaccante potrebbe utilizzare proprio questo sistema per sapere quando sei online e qual è il tuo indirizzo IP (lo stesso vale se inizi una chat su IRC).
Un'altra cosa che non si può escludere è che il tuo attaccante utilizzi NetBIOS o altri sistemi di individuazione delle risorse di rete, effettuando per esempio una scansione di una certa classe di IP alla ricerca di una macchina che si chiami "Giulio" (è vero che l'indirizzo è dinamico, ma quasi sempre è all'interno di un certo range...). Questo però richiederebbe un po' di tempo, e a quanto scrivi, gli attacchi avvengono subito dopo la connessione.
Potrebbe poi essere il tuo computer a segnalare in qualche modo all'attaccante la sua "posizione" in Rete: sei sicuro di non avere un virus o un trojan? O magari un keylogger che invia all'attaccante i dati raccolti durante la sua giornata di intercettazioni?
Inoltre, visto che non specifichi le porte in questione, bisogna anche prendere in considerazione l'idea che non si tratti affatto di un attacco, ma di una qualche normale attività di rete (qualche programma che usi, o il router della tua rete...).

TASTI DOLENTI

Nel nr.16 avete riportato un simpaticissimo elenco di "messaggi presi in considerazione da Microsoft per windows3000".
A proposito del punto 4 "Premi un tasto qualsiasi....no,NO,NO,NO QUELLO NO!" posso assicurarvi che grazie a Compaq con la nuova serie EVO ePC è già stato printamente implementato con l'attuale WindowsXP.
Utilizzando Partition Magic 8 (ma anche con altri programmi), se qualche cosa non funziona nel ridimensionamento delle partizioni al Reboot della macchina il programma chiede inutilmente di premere un qualsiasi tasto per interrompere ma.....la stupenda interfaccia solo USB per mouse e tastiera non fa vedere la tastiera quindi....si può premere qualsiasi cosa ma il sistema inesorabilmente si blocca.
Soluzione: smontare il disco fisso ed inserirlo in un volgare PC con tastiera tradizionale che viene sentita regolarmente al boot.
Complimenti per la simpaticissima rivista!

Andrea Sommaruga

HOT!

MANI LIBERE PER MITNICK

In questi giorni Kevin Mitnick, quello che è probabilmente il cracker più famoso del mondo, ha terminato di scontare la sua bizzarra ma commisurata pena, che lo ha tenuto lontano, per tre anni, da telefoni cellulari e connessioni a Internet.
L'ormai quasi quarantenne violatore di sistemi informatici, talmente abile e famoso dall'avere ispirato scrittori e registi per la figura dell'"hacker letterario", ha cominciato la sua carriera da adolescente, con un'impresa di tutto rispetto: la violazione di COSMOS, il sistema utilizzato da Bell, la principale compagnia telefonica statunitense, per la gestione della documentazione sulle chiamate. Pochi anni dopo, fu il turno di ARPANet, la rete telematica militare che fu il nucleo originario dell'attuale Internet. Impresa dopo impresa, si arriva alla metà degli anni '90, quando il fugace cracker viene arrestato. La lista delle sue violazioni è interminabile e misteriosa: e anche ora che il caso è, almeno per il momento, chiuso, molti segreti, ancora inviolabili, sono legati alla sua carriera.



Bufale via cellulare

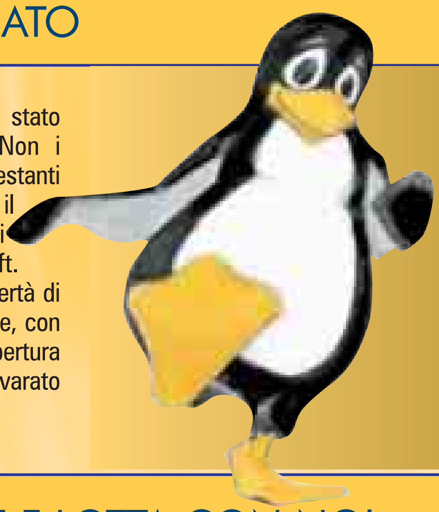
Ancora falsi allarmi via Sms. Questa volta si vocifera di una chiamata, proveniente dal misterioso NYK, che, se ricevuta, cancellerebbe i codici IMEI del cellulare, rendendolo inutilizzabile. A parte l'atmosfera da film cyberpunk anni '80, non c'è null'altro di interessante in questa segnalazione, che è completamente falsa. Seppure il messaggio millanti conferme da parte di Motorola e Nokia, inutile dire che nessuna delle due celebri case produttrici ne sa nulla.

VERME MANGIA VERME

Si è diffuso recentemente in Rete un nuovo worm, conosciuto come Sahay, concepito apparentemente allo scopo di distruggere un altro worm, Yaha. Ma non solo. La simpatica creaturina, già che passa da quelle parti, si spedisce in giro e tenta di infettare tutti gli eseguibili. Ma andiamo per ordine. Il worm si presenta in forma di salvaschermo, veste tutt'altro che nuova per la diffusione di un virus, dal nome di MathMagic.src. Eseguire questo file porta alla creazione automatica dello script yahasux.vbs (un nome che è tutto un programma) e al suo invio a tutti gli indirizzi della rubrica. Quindi passa a infettara qualsiasi file di estensione .exe. E, incidentalmente, ripulisce, seppure in maniera grossolana, l'hard disk dall'eventuale presenza del già citato Yaha.
Corre voce (incontrollata ma plausibile) che l'autore di tale file sia una delle poche viruswriter donna in circolazione, Gigabyte. L'indizio che lo fa pensare sarebbe la "signature" del virus, ovvero il classico messaggino nascosto all'interno del codice, che recita, più o meno: "Saluti. Apparentemente sei stato infettato da Yaha.K. Ma questo virus è stato scritto da un imbecille che SCRiVe CoSì, mi ha pasticciato il sito Web e mi ha rotto parecchio le scatole. Quindi ti ho disinfettato. Ma tranquillo, siccome non voglio portarti via nulla, ti ho lasciato un altro virus (Win32.HLLP. YahaSux) in cambio".

PINGUINI AL SENATO

L'intervento di Bill Gates al Senato è stato salutato da una folla di pinguini. Non i simpatici pennuti dei ghiacci, ma manifestanti appositamente travestiti, a simboleggiare il software libero come alternativa ai progetti altisonanti del fondatore di Microsoft. L'invocazione era quella a una maggior libertà di scelta verso soluzioni sicure e open source, con un po' di polemica verso il progetto di "apertura parziale" del codice di Windows appena varato da Bill Gates.



SETI@HOME VIVE E LOTTA CON NOI

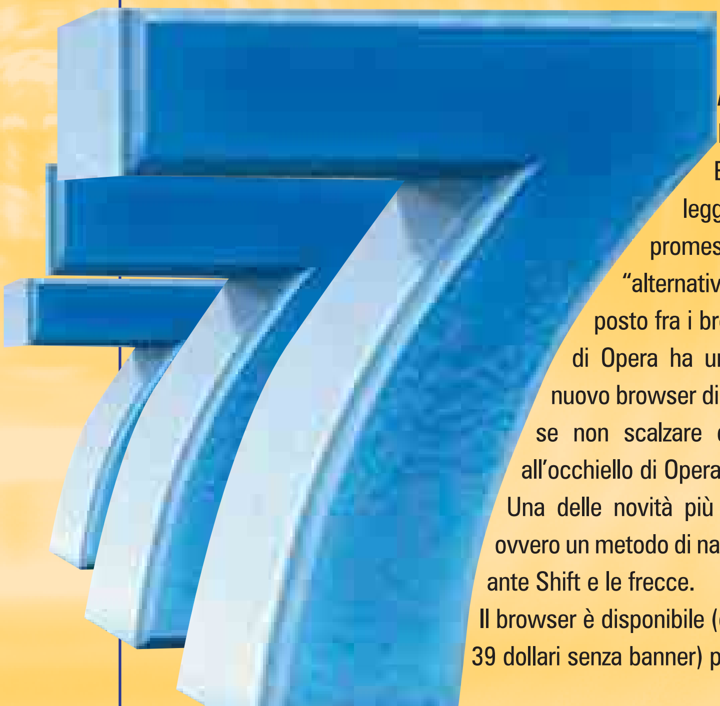
Non è una novità, ma può essere interessante ricordarne l'esistenza: si tratta del progetto SETI@HOME dell'Università di Berkeley, che sfrutta la potenza di calcolo dei computer connessi ala Rete e momentaneamente inattivi per analizzare i dati provenienti da un radiotelescopio, alla ricerca di presenze di extraterrestri nello spazio. Installando un apposito client sul proprio computer, si potrà partecipare a questo affascinante progetto, non troppo dissimile da un salvaschermo.
Il software e tutte le informazioni del caso sono reperibili presso http://setiathome.ssl.berkeley.edu/



AOL TIME WARNER NELLA POLVERE

La creatura nata dalla fusione del celebre provider statunitense con il gigante dei media sta perdendo qualche colpo, per usare un eufemismo. Le perdite relative al 2002 sfiorano i 100 milioni di dollari, un numero ragguardevole anche per le grandi cifre in ballo nel mercato finanziario americano. Questa batosta segue al "modesto" passivo del 2001, che era di "appena" 5 miliardi di dollari, e le dimissioni dei più alti vertici della dirigenza, fra cui il guru dei media Ted Turner, che ne era vicedirettore.

OPERA 7 ARRIVA SU WINDOWS



E finalmente disponibile la versione definitiva di Opera 7, che ha tutte le intenzioni di scalzare seriamente Explorer dal suo trono. Più veloce, più leggero e più funzionale: queste sono le promesse dei produttori del popolare browser "alternativo", che le statistiche vedono al terzo posto fra i browser più diffusi al mondo. La scalata di Opera ha una sola nuvola all'orizzonte: Safari, il nuovo browser di Apple, che potrebbe far indietreggiare se non scalzare del tutto dal mercato uno dei fiori all'occhiello di Opera, la versione per Mac.
Una delle novità più interessanti è la Spatial Navigation, ovvero un metodo di navigazione all'interno della pagina mediante Shift e le frecce.
Il browser è disponibile (gratuitamente in versione adware, o a 39 dollari senza banner) presso www.opera.com.

COLLABORARE È UN CRIMINE

Un tecnico informatico statunitense che aveva messo a disposizione alcune macchine della rete scolastica a lui affidata per un progetto di "distributed computing", ovvero, come il già citato SETI@HOME:, un progetto che permette di utilizzare le risorse di un computer attraverso la Rete, quando esso è inattivo, per effettuare calcoli complessi. E l'accusa non è lieve: furto di risorse informatiche e violazione della sicurezza, per avere installato un software di terze parti. Essendo la pena cumulativa per ogni computer sul quale è stata operata la modifica, si arriva allo sbalorditivo totale di 120 anni. E addirittura a un tentativo di richiesta di risarcimento di 415.000 dollari, che sarebbe il costo della banda totale occupata dai vari client, richiesta fino ad ora rigettata.
Ovviamente, attorno a questo caso è sorta una feroce polemica. La colpa viene attribuita alla rigidità delle leggi statunitensi in materia di sicurezza informatica, espresse in termini talmente grossolani da creare casi limite, come questo. E all'assurdità dell'accusa di installazione illecita di software di terze parti in un ambiente, come quello universitario, che vede violazioni continue e tollerate a tale norma.

HOT!

DOCUMENTI FIRMATI MICROSOFT

Microsoft è in procinto di rilasciare un addon per Word 2000 e 2002 (Xp, per intenderci), volto a consentire l'applicazione della firma elettronica, a norma di legge - ricordiamo che l'Italia ha una interessante seppur ancora embrionale legislazione in materia - ai documenti prodotti dal popolare editor. Un servigio utile e una manovra accattivante da parte dei signori di Redmond, visto che nessun ente pubblico potrà prescindere dal dotarsi di uno strumento di elaborazione testi che supporti tale funzionalità. Come dire: nel prossimo futuro, niente appalti o concorsi pubblici per la fornitura di software, senza il supporto alla firma digitale. E l'egemonia di Microsoft, già minata dall'insinuarsi di Linux negli enti pubblici, non potrebbe forse reggere una ulteriore batosta. Ma neppure le imprese o i liberi cittadini che hanno necessità di un dialogo regolare, magari in via telematica, con le strutture pubbliche potranno (o vorranno, perché no) fare a meno del supporto alla firma digitale.
Una precisazione doverosa: date le caratteristiche intrinseche della firma elettronica, volte a garantire non solo l'autenticità, ma anche l'integrità di un documento, tutti i documenti che presentano parti attive, quali macro, saranno resi "statici" e salvati in copia per la firma, senza pregiudicare l'originale né inficiare la validità della firma elettronica.

5 EURO DI MUSICA OMAGGIO

Durerà fino al 21 marzo un'iniziativa, chiamata Digital Download Day Europe, patrocinata dalla major discografiche, valido per utenti italiani, spagnoli, francesi, olandesi, tedeschi e britannici. Ogni nazione ha un partner locale (Tiscali per l'Italia) che fornirà l'account omaggio a OD2, dove, una volta connessi, potremo scegliere fra circa 150mila brani, ottenuti in licenza dai più grandi colossi della musica.

HOT!

5 GBYTE IN TASCA

Un rivale si profila all'orizzonte delle memorie rimovibili: StorCard, un dispositivo in grado di archiviare fino a 5 Gbyte di dati e delle stesse dimensioni di una carta di credito. In qualche modo si è voluto creare un anello di congiunzione fra il vecchio floppy e le nuove memorie rimovibili: il disco magnetico viene letto da un dispositivo detto StorReader, molto simile a un floppy drive, che verrà integrato sia sui desktop (mediante USB) che sui notebook (PC Card Type II).
La velocità di lettura è intorno ai 5 Mbyte al secondo; è presente un supporto per la criptazione dei dati e, in generale, il dispositivo si presenta molto adatto al supporto per la firma elettronica, soprattutto per la sua forma peculiare che permette di integrare una banda magnetica.
Le prime StorCard usciranno nel formato da 100 Mbyte, ad un prezzo di circa 15 dollari, mentre il lettore si aggirerà attorno ai 100 dollari.



VERISIGN DALLA LINGUA LUNGA

Nell'ultima mail di comunicazione agli utenti, Verisign si è lasciata sfuggire una distrazione non di poco conto: l'elenco completo, in chiaro, di tutti i possessori di domini .org, circa 87.000 persone. L'elenco oltretutto appesantiva notevolmente il messaggio, portandolo a circa 2 Mbyte. Alti si sono levati gli scudi degli utenti contro VeriSign: un database di 87.000 nomi di possessori di domini.org ha un valore pressochè incalcolabile, per uno spammer.

PC: SCONTO PER SEDICENNI

Nulla di eclatante, ma meglio che niente: il governo italiano ha stanziato una somma pari a circa 70 milioni di euro, che dovrebbero aiutare circa mezzo milione di giovani italiani a acquistare un Pc, per un contributo pro capite che si aggira attorno ai 150 euro a testa, nell'ambito di una operazione tesa all'ampliamento dell'alfabetizzazione informatica. Per ora l'intera operazione è ancora in attesa del beneplacito del ministro Tremonti, ma, una volta attivata, un sito e un call center permetteranno di avere maggiori informazioni e sottoscrivere la propria adesione all'offerta. Ai fortunati prescelti, ricadenti nei requisiti stabiliti per lo sconto, verrà inviato una sorta di codice PIN, unico e personale, che attiverà lo sconto per una volta sola e poi sarà disattivato (per evitare abusi). Una formula più scarna e più lineare del precedente "computer per studenti", su cui ben pochi sono riusciti a mettere le mani (si parla di non più di diecimila studenti), soprattutto per le non indifferenti garanzie bancarie richieste.



GRID COMPUTING ALLO SCOPERTO

Un sistema per l'utilizzo delle risorse di calcolo molto interessante, riservato fino a ieri a aboratori e centri di ricerca, vede ora una rinascita nel mercato enterprise. Il grid computing non è altro che l'aggregazione e la distribuzione di risorse di calcolo mediante una rete di server e workstation, così come accade normalmente per la rete idrica o elettrica, che consente quindi alle aziende di poter disporre proprio di quella determinata quantità di risorse quando più ne ha bisogno, senza sovraccaricarsi di dispositivi con relativi budget altissimi o, peggio ancora, scoprire di avere a disposizione risorse insufficienti.
Le tecnologie di grid computing sono sviluppate da IBM, in collaborazione col progetto (naturalmente open source) Open Grid Services Architecture (OGSA). Per permettere la diffusione di questo progetto nell'impresa, sono stati studiati dieci "pacchetti" personalizzati: trasporti, finanza, enti pubblici e via dicendo, su ognuno dei quali il sistema di distribuzione è stato ottimizzato in rapporto all'utilizzo previsto.

PROROGA ALL'ICANN

Il noto (per non dire famigerato) ente di supervisione dei domini Internet sta per ottenere una proroga di tre anni del contratto che lo lega al Ministero del Commercio degli Stati Uniti. La notizia potrebbe anche lasciare freddini, se non fosse che l'istituto rappresenta una sorta di "governatore dei domini" di tutto il mondo, e che più volte è stato al centro di polemiche per la sua dipendenza da tale ministero. L'impressione è che l'Icann tema di non riuscire ad affermarsi autonomamente senza tale importante supporto, aggravando ulteriormente i già non indifferenti disservizi a carico della rete mondiale.

ICANN

HOT!



VIDEOCAMERA CON HARD DISK

Samsung ha presentato ITCAM-7, una videocamera provvista di hard disk da 1,5 Gbyte, in grado di memorizzare video, immagini, audio e musica, con lettore MP3 e MPEG incorporati.
E' presente inoltre uno slot Memory Stick, per trasferimento dati e memorizzazioni supplementari. Il video è riproducibile sia sul display LCD che in uscita, su TV, e da TV può anche effettuare registrazioni. L'hard disk può essere utilizzato anche come dispositivo portatile, per il trasporto dati e per la riproduzione di file multimediali.

ORACLE WIRELESS

Sta per essere introdotto in fase di test un application server dedicato a applicazioni per dispositivi mobili, denominato Oracle 9i Application Server Wireless, con il support a XHTML 2.0 e J2ME.
Il vantaggio di questo sistema è l'interscambiabilità: ogni server elaborerà on the fly i dati per adattarli allo specifico dispositivo, senza bisogno di creare applicazioni differenziate per le diverse categorie di prodotti.

NVIDIA PROFESSIONALE

Una nuova serie di GPU, Quadro FX, è il nuovo fiore all'occhiello di Nvidia per quanto riguarda il mercato delle workstation. Due serie, FX1000 e FX 2000, con unità di calcolo in virgola mobile a 128 bit, pipeline di rendering a 8 stadi e motore grafico programmabile. Le memorie utilizzate sono le nuove DDR-II. E' presente il supporto all'antialiasing a pieno schermo, e la risoluzione massima possibile è di 3840x2400. I prezzi si prevedono attorno a 1300 dollari per le FX1000 e 2000 per le FX2000.

The way it's meant to be played
NVIDIA

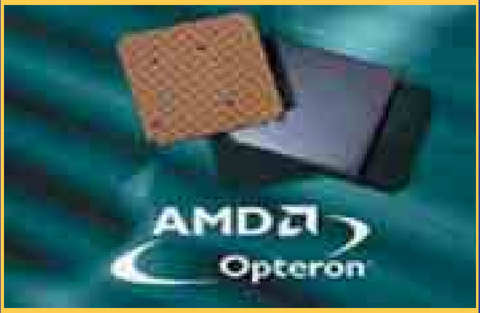
LINDOWS VA IL VERSO A WINDOWS XP

Linux vuole entrare nei salotti, e per farlo non risparmia colpi, puntando sul multimediale né più né meno di quel che fa Microsoft con i suoi sistemi operativi consumer. Nascono così i Lindows Media Computer, provvisti di lettore CD e DVD, con interfaccia del tutto simile a quella di XP Media Center, per la riproduzione di DVD, CD, MP3 e Video CD. E l'offerta è economicamente allettante: si parla di 330 dollari, monitor escluso, in offerta online su iDOTpc (www.idot.com). Si tratta di un prodotto simile al già noto PC con LindowsOS, con processore Via C3 da 933 MHz, ma il boot è velocissimo e l'interfaccia di avvio presenta a pieno schermo il menu di accesso alla riproduzione multimediale. Naturalmente, è presente e accessibile anche LindowsOS 3.0.
A onor del vero, si tratta di un prodotto più "rozzo" e provvisto di meno funzionalità del suo equivalente Windows: ma i costi sono estremamente inferiori, e alcuni funzioni utili ma non indispensabili come il telecomando lasciano volentieri il passo a parecchie centinaia di euro risparmiati.

LindowsOS

NOVITÀ DA AMD

Sono in arrivo i nuovi modelli della serie Athlon XP, 3000+ e 3200+, previsti rispettivamente per il 10 febbraio e la metà dell'anno. Ambedue saranno basati sul nuovo core, dal nome in codice Barton, a 0,13 micron, con cache L2 da 512 KB, che vuole essere un trampolino di lancio verso l'atteso Athlon 64, il primo chip in assoluto per desktop e notebook con supporto 64 bit. La sua data d'uscita è però ulteriormente slittata: è ora atteso per settembre. Mentre è questione ormai di pochi mesi (22 aprile) per Opteron, il chip a 64 bit per server e workstation, che va a porsi in diretta concorrenza con Itanium di Intel.
L'appuntamento successivo è quello con la tecnologia a 90 nanometri, che sostituirà nel 2004 gli 0.13 micron sui modelli denominati in codice Odessa, San Diego e Athens (rispettivamente Mobile Athlon 64, Athlon 64 e Opteron).
Sia Opteron che Athlon 64 si basano sull'architettura ibrida AMD a 32/64 bit denominata x86-64, che consente di eseguire applicazioni a 64 e 32 bit senza cali di prestazioni in nessun senso. AMD punta molto soprattutto su Athlon 64, ritenendo che l'architettura a 64 bit possa rappresentare una soluzione interessante anche per il mercato consumer.



SORRIDI, SEI SU BIOMETRIC CAMERA

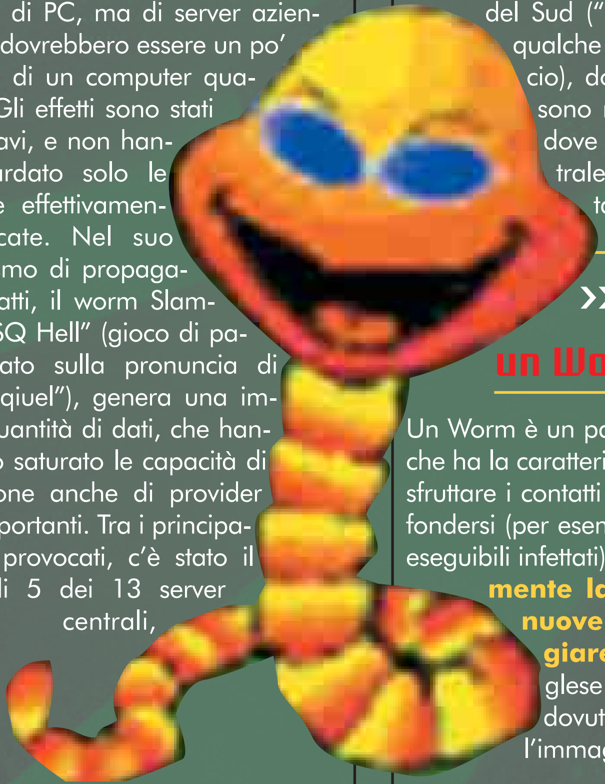
La biometria, un pilastro importante per lo sviluppo di applicazioni relative alla sicurezza e alla firma digitale, è stata messa in pratica all'aeroporto di Sidney, dove chioschetti denominati SmartGate controlleranno che la faccia del passeggero corrisponda effettivamente a quella raffigurata sul passaporto. E lo scanner non si fa ingannare da età, taglio di capelli, barba o baffi più o meno presenti.

COME FUNZIONA, CHE DANNI HA PROVOCATO E COME SI POTEVA EVITARE…

Slammer: L'INFERNO DI SQL

376 caratteri: queste sono le dimensioni del Worm che per due giorni ha messo in ginocchio la Rete.

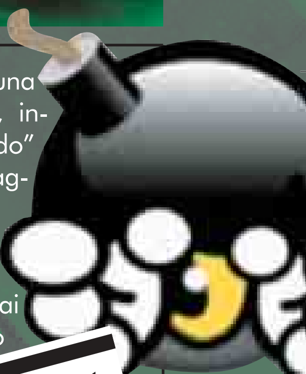
Tra il 24 e il 25 gennaio scorsi, la Rete è stata scossa dall'assalto di un nuovo Worm, che attacca Microsoft SQL Server. In meno di due giorni, sono stati infettati circa 120.000 sistemi. E non stiamo parlando di PC, ma di server aziendali, che dovrebbero essere un po' più sicuri di un computer qualunque. Gli effetti sono stati molto gravi, e non hanno riguardato solo le macchine effettivamente attaccate. Nel suo meccanismo di propagazione infatti, il worm Slammer, o "SQ Hell" (gioco di parole basato sulla pronuncia di SQL, "esquiel"), genera una immensa quantità di dati, che hanno presto saturato le capacità di trasmissione anche di provider molto importanti. Tra i principali danni provocati, c'è stato il blocco di 5 dei 13 server DNS centrali, dai quali dipende la risoluzione degli indirizzi Internet.



Inutilizzabili anche 13.000 sportelli bancomat della Bank Of America e, dalle nostre parti, 14.000 sportelli delle Poste e parecchi servizi offerti da Libero. Peggio è andata a India, Cina e Corea del Sud ("ben gli sta", penserà qualche appassionato di calcio), dove parecchi provider sono rimasti inaccessibili, e dove anche qualche centrale telefonica è saltata.

>> Ma cos'è un Worm?

Un Worm è un particolare tipo di virus, che ha la caratteristica di non limitarsi a sfruttare i contatti "occasionali" per diffondersi (per esempio dallo scambio di eseguibili infettati), ma **sfrutta attivamente la rete per cercare nuove vittime da contagiare**. Il nome, che in inglese significa "verme", è dovuto probabilmente all'immagine di questo codice malevolo che corre da una parte all'altra della Rete, ingrandendosi e "crescendo" sempre più a ogni passaggio. Un Worm può trasmettersi da server a server, oppure appoggiarsi anche ai computer "client", e può propagarsi in vari





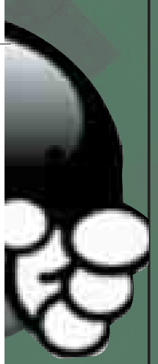
Il fatto che tra le principali vittime in Italia ci fossero le Poste, che hanno avuto 14.000 sportelli paralizzati, ha fatto pensare a un attacco terroristico. Probabilmente non è così, e questo è ancora peggio: se ciò che abbiamo visto sono le conseguenze di un'infezione casuale, cosa succederà quando qualcuno sferrerà un attacco mirato e coordinato?



modi: attraverso richieste mal formattate, che fanno impazzire il server, oppure sfruttando la posta elettronica, i sistemi di chat.

Oltre ai danni che può provocare sui sistemi che infetta, un Worm è sempre dannoso per l'intera Rete: **il suo meccanismo di diffusione infatti fa sì che il ritmo di attività cresca in modo esponenziale**, andando a intasare tutta la banda disponibile.

>> Come funziona

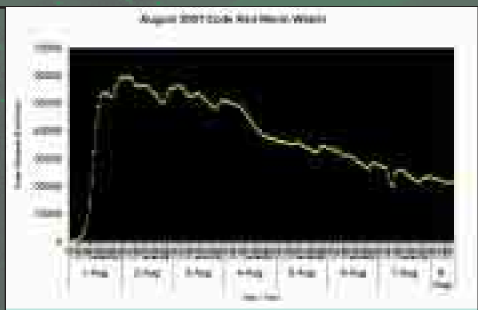


SQL Server può ricevere connessioni dai client in due modi: attraverso una richiesta effettuata via NetBIOS, oppure via Internet. **In ogni caso, la porta 1434 rimane aperta per ricevere messaggi UDP**: inviando un messaggio di un singolo byte alla porta 1434, infatti, il client potrà scoprire in modo dinamico quale sia la modalità più adatta al collegamento. **Inviando messaggi più lunghi di un byte, SQL tenterà di aprire una chiave di registro usando i dati rimanenti**. Slammer agisce proprio in questo modo: inviando un particolare pacchetto di 376 byte, trasforma il server attaccato in una nuova base di partenza per cercare e attaccare altre vittime sulla rete. In questo modo, l**a banda e le risorse del computer vengono presto saturate dall'enorme quantità di richieste e dati trasmessi**.

Fortunatamente, Slammer agisce solo in memoria: non crea e non cancella dati sul disco del computer attaccato.



I sistemi vulnerabili sono i server con Microsoft SQL oppure i computer personali che montano Microsoft SQL Desktop Edition, una versione ridotta di SQL compresa in molti software di sviluppo o di amministrazione, tra cui anche certe edizioni di Office XP, Visio, Visual Studio .NET, Visual Basic .NET, Encarta Class Server e altri. Una lista completa dei software Microsoft che installano MSDE in modo predefinito o a richiesta è disponibile all'indirizzo : www.microsoft.com/technet/treeview/default.asp?url=/technet/security/MSDEapps.asp

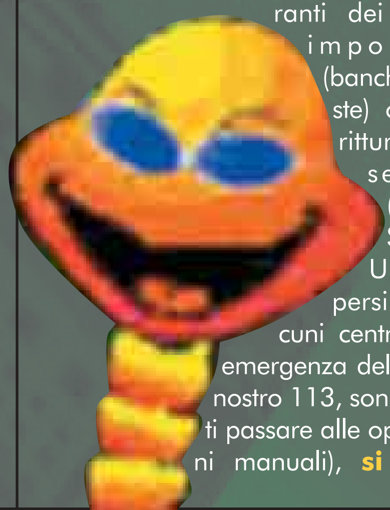


Il grafico della diffusione del worm Code Red 2, effettuato in base alle scansioni osservate da indirizzi IP diversi. Notare come in poche ore si passi da alcune centinaia, a decine di migliaia di computer infettati.

>> La solita "tragedia annunciata"

Finita l'emergenza, è subito partita la caccia ai responsabili: quando l'intera Internet rallenta, e vengono resi inoperanti dei servizi importanti (banche, poste) o addirittura essenziali (negli Stati Uniti, persino alcuni centralini di emergenza del 911, il nostro 113, sono dovuti passare alle operazioni manuali), **si cerca subito qualche testa da far cadere**. E gli occhi di tutti si sono puntati sugli amministratori di sistema, che **avrebbero dovuto avere installato più di sei mesi fa la patch** che risolve il baco sfruttato da Slammer.





La patch è infatti stata rilasciata da Microsoft **fin dal 25 luglio 2002**, quando i principali siti di security riportarono la notizia dell'update indicandolo come "aggiornamento critico", dovuto a un "rischio molto alto". Ma forse a fine luglio molti amministratori di sistema erano già al mare.

E probabilmente erano in vacanza anche **verso la metà di maggio, quando è stato dato il primo avviso della presenza di un possibile baco di buffer overflow in SQL Server** (17 maggio 2002, http://www.nextgenss.com/vna/ms-sql.txt). Questo articolo già descriveva una possibile soluzione al problema, basata sulla impostazione di una serie di regole sul firewall, mirate a filtrare i pacchetti UDP destinati alla porta 1434.

>> Solo colpa loro?

In un modo o nell'altro, questa è l'idea che Microsoft tende a far passare, ma non tutti sono d'accordo. Qualche amministratore di sistema infatti, fa notare che –se è vero che la patch che risolve il problema sfruttato da Slammer è disponibile da luglio– bisogna anche dire che **questa patch non è mai stata distribuita come modulo a sé stante, ma solo all'interno del Service Pack 3**, e ci sono diversi (validi?) motivi per non installare un Service Pack di Microsoft. Innanzi tutto c'è la questione delle licenze, che sono diverse da quella della prima versione del prodotto, e sono ben più restrittive. Qualcuno potrebbe non condividere la licenza d'uso (EULA, End User License

COME FUNZIONA, CHE DANNI HA PROVOCATO E COME SI POTEVA EVITARE…

BREVE STORIA DEI WORM

Novembre 1988: il grande worm di Internet



Robert Morris, uno studente della Cornell University (oltre che figlio di un pezzo grosso dell'NSA), rilascia il primo worm, che per anni rimarrà famoso semplicemente come "The Big Internet Worm". Nel giro di poche ore, contagerà circa 6000 computer, che all'epoca rappresentavano il 10% circa dell'intera popolazione della Rete.

Marzo 1999: Melissa

Il primo virus a diffusione massiccia che sfrutta i problemi di sicurezza insiti in Outlook e Outlook Express, e usa la rubrica degli indirizzi per replicarsi a tutti i destinatari. Alcune varianti poi, allegano ai messaggi informazioni prese a casaccio dall'hard disk, provocando parecchie situazioni imbarazzanti. L'infezione comincia di venerdì, nel giro di poche ore arriva in tutto il mondo. Ma è solo al successivo lunedì, alla riapertura degli uffici, che i danni si fanno davvero imponenti. Persino Microsoft è costretta a spegnere il suo sistema di posta.

Maggio 2000: I love you

Dalle Filippine, parte LoveLetter.VBS, il virus più dannoso mai registrato fino a quel momento. Ha in comune molto con Melissa, ma il codice sfrutta meglio le vulnerabilità del sistema di scripting di Outlook, e fa molta più presa anche nella psiche umana: chi non aprirebbe una lettera che dice "ti amo"?

Luglio 2001: Code Red

Dopo aver fatto incetta tra i computer personali, nel 2001 i Worm sono tornati ad attaccare i server con Code Red, diventato famoso come "il Worm più costoso della storia di Internet". Quando fu individuato, aveva già contagiato 20.000 computer. "Codice Rosso" attacca il Web server di casa Microsoft (Internet Information Server) e cerca di replicarsi allo stesso modo. Il traffico generato dalle scansioni effettuate dai server infettati, spesso connessi a Internet con collegamenti a larga banda, ha messo in ginocchio più di un'azienda. In più, Code Red impianta una backdoor che consente l'amministrazione remota di alcune funzioni del server.



Settembre 2001: Nimda

Senza neanche il tempo di riprendersi da Code Red, dopo soli due mesi la Rete è stata scossa da un'altra minaccia: Nimda. In sé, il programma virale non mostrava particolari innovazioni; anzi, sfruttava bachi di sicurezza ben noti, molto vecchi, quasi dimenticati. La sua particolarità, è che li sfruttava tutti assieme, usando canali diversi: Nimda infatti poteva sfruttare bug di IIS, Explorer, della condivisione file di Windows e di Outlook per spargere l'infezione tra client e server e viceversa, con unamicidiale promiscuità, fino a quel momento mai vista.



Agreement), e quindi non volerla installare. Microsoft non è nuova a queste bizzarrie con le licenze: **la prima versione del prodotto è accompagnata da una licenza piuttosto permissiva, che viene però modificata in modo restrittivo a ogni Service Pack**. Per ultimo, **accade spesso che i Service Pack modifichino le impostazioni di sicurezza di un server**, cosa che non fa mai piacere a un amministratore di sistema.

Per tutti questi motivi, molti molti amministratori di sistema adottano la politica: "se funziona, non lo aggiornare", anche se questa li espone a problemi come quello manifestatosi nelle scorse settimane. Quello che molti amministratori di sistema chiedono è una raccolta di singoli aggiornamenti e patch, che ciascuno può decidere di installare in modo indipendente.

Insomma, per quanto riguarda il processo degli aggiornamenti di sicurezza, la relazione tra Microsoft e i suoi clienti sembra avere qualche problema. Pensate poi che, **persino Microsoft non aveva applicato la patch ad alcuni dei suoi server interni** che svolgevano compiti molto importanti, come quelli dedicati all'autenticazione di Windows XP.



REALIZZARE UN PROGRAMMA CHE NASCONDE TESTI IN UN'IMMAGINE

COME TI NASCONDO IL FILE



In passato, il fatto di nascondere un messaggio in un altro aveva un vago sentore di zolfo e magia, ma anche oggi non è chiaro a tutti come possa funzionare questo processo. Vediamolo insieme!

Il termine Steganografia deriva dal greco e significa "scrittura nascosta".

La steganografia ha varie forme; in informatica si utilizza in genere la steganografia sostitutiva, ovvero quella in cui si sostituiscono dei dati per nasconderne altri. Queste sono tecniche utili per **occultare testi o altro all'interno di documenti "insospettabili" quali, per esempio, immagini, audio o filmati**. Visti i sempre più frequenti discorsi sull'insicurezza in Internet, la steganografia consente di trasmettere documenti riservati o personali mantenendoli tali e non mettendoli alla mercé di chiunque.

Passando subito alla pratica (per la teoria della steganografia, consigliamo una ricerca sui vari motori di ricerca in Internet) si esamineranno in questo articolo i principi di base per realizzare un programma di steganografia.



>> Nascondere i dati

Qualsiasi documento informatico su qualsiasi piattaforma, appare al computer come sequenza di byte. Sia esso un testo o un programma, altro non è che una sequenza di caratteri. Dato questo per scontato, si può partire dicendo che se si vuole celare un documento all'interno di un'altro si deve trovare un compromesso: **o si aggiunge qualcosa o si modifica qualcosa**.

Il sistema più efficiente e meno evidente consiste nel codificare un documento all'interno di una immagine. Anche questa è che una sequenza di byte. Prendendo in esame una immagine a colori, generalmente a 24 bit per pixel, si hanno 3 byte per ciascun pixel. Ugni byte rappresenta il livello del colore primario cui fa riferimento.

Quindi, un byte indicherà il livello della componente rossa, uno il verde e uno il blu i quali sono i colori luce fondamentali.

Dopo avere detto che ogni pixel ha 3 byte, che indicano ciascuno le componenti cromatiche, va anche detto che una variazione dei valori dei singoli byte corrisponde a una variazione dell'immagine. Se essa è minima, è impercettibile all'occhio umano.

Ecco perchè si modificherà solo l'ultimo bit di ciascun byte dell'immagine per inserirvi un bit del testo da nascondere.

>> Un esempio pratico

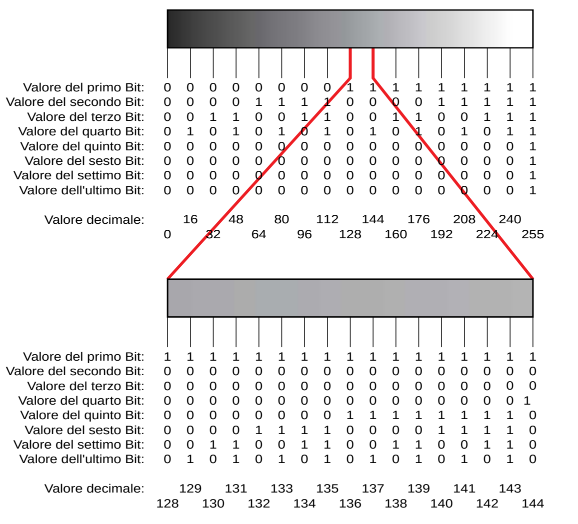


L'immagine ha vari byte che la compongono, i primi 8 che si analizzano hanno (per esempio) i seguenti valori:

[145] [211] [85] [99]
[77] [177] [248] [218]

La prima lettera del testo da nascondere è la lettera "C" che ha un valore Ascii 67 che in binario corrisponde a 0100000011.

Scomponendo in bit i byte del-



Ogni byte (nelle colonne) indica il livello del colore primario cui fa riferimento. Sopra, i vari byte che indicano varie intensità di colore. Nella parte inferiore si nota che al variare dell'ultimo bit di una sola unità, corrispondo variazioni di tono impercettibili. Basandosi su questo fatto è possibile scomporre un carattere di testo nei bit corrispondenti secondo la codifica ASCII e quindi modificare l'ultimo bit dei byte relativi ai vari pixel dell'immagine per inserirvelo.

Il programma di codifica

```
Definisci la variabile "Testo"
Definisci la variabile "Immagine"
Definisci la variabile "NuovaImmagine"
Definisci la variabile "Header" ##Conterrà la parte
di Header dell'immagine originale##
Leggi il contenuto del file di testo mettilo nella
variabile "Testo";
Leggi il contenuto del file di immagine, tralascia la
parte di Header, metti la parte dati nella variabile
"Immagine"
```

In questa fase, occorre conoscere la struttura del formato immagine usato. Per semplificarsi la vita, si può lavorare solo su formati "grezzi" come per esempio il formato "RAW" di Photoshop, che non ha Header.

```
Se la lunghezza del file di testo è maggiore di (lunghezza del file di immagine / 8) avvisa che il file
di immagine è troppo piccolo quindi esci dal programma.
Metti "1" nella variabile "ContatoreTesto"
Metti "1" nella variabile "ContatoreImmagine"
Ripeti per il numero di caratteri della variabile
"Testo"
  Metti il valore numerico del carattere N°
("ContatoreTesto") della variabile "Testo" nella
variabile "BitCar"
  converti il valore di "BitCar" in binario
  metti "1" nella variabile "ContaBit"
Ripeti 8 volte
  se il valore del carattere N° ("ContaBit") della
variabile "BitCar" è uguale a "0"
      metti il valore del carattere N°
"ContatoreImmagine" nella variabile "ByteImmagine"
      metti (tronca ("ByteImmagine"/2)*2) nella variabile "ByteImmagine"
      converti la variabile "ByteImmagine" nel carattere corrispondente al suo valore numerico
```

Sarà necessaria una funzione esterna

```
  altrimenti
      metti il valore del carattere N°
"ContatoreImmagine" nella variabile "ByteImmagine"
      metti (tronca ("ByteImmagine"/2)*2)+1 nella
variabile "ByteImmagine"
```

Qui in realtà occorrerebbe verificare se il valore risultante è superiore a 255, in tal caso avremmo un errore siccome non posiamo avere un carattere con valore superiore a 255!

```
      converti la variabile "ByteImmagine" nel
carattere corrispondente al suo valore numerico
```

Sarà necessaria una funzione esterna

```
    fine "se"

    Aggiungi 1 alla variabile "ContatoreImmagine"
    ##in seguito uso il successivo carattere grazie
all'impiego di questo contatore##
    Aggiungi 1 alla variabile "ContaBit"
    ##in seguito uso il successivo carattere grazie
all'impiego di questo contatore##
  Fine ripeti ##Era: Ripeti 8 volte##
Fine ripeti ##Era: Ripeti per il numero di caratteri
della variabile "Testo"##
```

Giunti a questo punto, la variabile "Header" contiene ancora la parte di Header dell'immagine originale; la variabile "NuovaImmagine" contiene parte dei dati immagine già codificati per contenere il testo; la variabile "Immagine" contiene i dati immagine originali. Ora si procede a scrivere il file della nuova immagine col testo codificato al suo interno.

```
Apri il file (nome del file) in scrittura
Scrivi nel file (nome del file) la variabile "Header"
Scrivi nel file (nome del file) la variabile
"NuovaImmagine"
Scrivi nel file (nome del file) la variabile "immagine" a partire da (carattere (lunghezza della variabile "NuovaImmagine") + 1)
Chiudi il file (nome del file)
```

La composizione delle immagini

I colori della luce sono il rosso, il verde e il blu; sommandoli in egual misura si ottiene luce bianca. Questo metodo, detto sintesi additiva, è quello usato per generare colori in tutti i dispositivi che emettono luce come i monitor e le televisioni. Se si guarda con una lente d'ingrandimento una televisione, si vedono distintamente le singole parti rosse, verdi e blu che opportunamente comandatye generano le immagini.

>> Questioni generali

Se avete avuto la pazienza di leggere tutta la sezione di programmazione, **siete pronti per realizzare il vostro programma di Steganografia col linguaggio che preferite**.

Come suggerito nel codice, occorrono delle funzioni esterne per vari scopi, quali la verifica dell'esattezza del nome del file secondo gli standard della piattaforma adottata, la conversione da numero decimale a binario e viceversa.

L'unico problema che si può incontrare sta nella codifica dei vari formati di file i quali possono avere degli Header che vanno lasciati inalterati se si vuole potere visualizzare l'immagine.

Tra i formati di file da usare, sono sconsigliati i formati che usano compressione (per esempio TIFF compresso in LZW, JPG) in quanto **il file sarebbe da interpretare prima di poterlo usare, e poi producono file molto piccoli**, che permettono di nascondere meno dati. Con-

Il programma di decodifica

```
Definisci la variabile "Testo"
Definisci la variabile "Immagine"
Leggi il contenuto del file di immagine, tralascia
la parte di Header, metti la parte dati nella
variabile "Immagine"
Metti "1" nella variabile "ContatoreImmagine"
##tiene conto di quale byte di immagine sto elabo-
rando sto esaminando##

Ripeti per il numero di caratteri della variabile
"Immagine"

  Metti 1 nella variabile "ContaTesto" ## Quando
questa variabile è uguale a 8 significa che ho
letto un carattere del testo ##
  Metti "" nella variabile "CarattereLetto" ##
Inizializzo o svuoto la variabile che contiene il
carattere letto ##

  Ripeti finchè ("ContaTesto" = 8)
     metti il valore numerico del carattere n°
"ContatoreImmagine" della variabile "Immagine"
nella variabile "NumCar"
     Se (tronca ("NumCar" / 2)) * 2 è uguale a
"NumCar" ## significa che l'ultimo bit era "0" ##
        metti "0" dopo la variabile "CarattereLetto"
     altrimenti
        metti "1" dopo la variabile "CarattereLetto"
     fine Se
     Aggiungi "1" alla variabile "ContatoreImmagine"
     Aggiungi "1" alla variabile "ContaTesto"
  Fine ripeti ## Ripeti finchè (ContaTesto = 8) ##

  Converti "CarattereLetto" da binario al carattere
corrispondente ## sarà necessaria una funzione
esterna ##
  Metti "CarattereLetto" dopo la variabile "Testo"
## la variabile "CarattereLetto" contiene un carat-
tere ascii, lo vado a scrivere dopo il contenuto
della variabile "Testo" che già contiene il testo
finora letto ##

Fine ripeti ##Era: Ripeti per il numero di caratte-
ri della variabile "Immagine"##

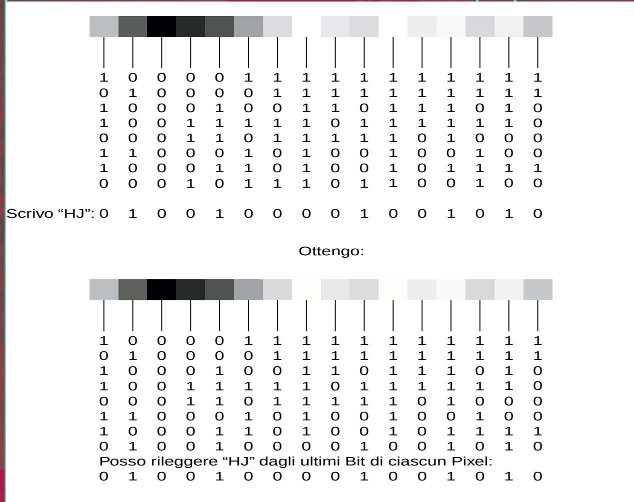
Apri il file (nome del file di testo) in scrittura
## Il nome del file potrebbe essere un nome stan-
dard, il nome dell'originale più un testo per iden-
tificarlo o un nome definito dall'utente. ##
  Scrivi nel file (nome del file di testo) la
variabile "Testo"
Chiudi il file (nome del file)
```

viene usare formati come il TIFF non compresso e il BMP i quali (dopo la sezione di header) scrivono i dati byte per byte. Per tutti coloro che non hanno familiarità con i formati grafici, il formato consigliato è il formato RAW (disponibile da diversi programmi quali per esempio Photoshop anche nella versione economica Photoshop Elements) dato che questo **scrive nel file solo i dati immagine**. Usando questo formato, occorre ricordarsi però le dimensioni in pixel dell'immagine, dato che esse non sono scritte nel file!

>> Conclusioni

Un programma di steganografia è un ottimo strumento per tenere nascosto ciò cha abbiamo di più privato, dalle lettere della morosa fino ai documenti aziendali più riservati. Va comunque detto che i dati scritti, una volta estratti, sono leggibili da chiunque anche con altri programmi di steganografia. Se si teme di avere vicino qualche curioso, può essere conveniente cifrare i testi usando un programma tipo PGP prima di inserirli nell'immagine. In questo modo, anche estraendo i dati, si dovrà lottare per tentare di leggerli e si avrà una ancor maggiore – per non dire totale – riservatezza.
Volendo, si può inserire nell'immagine e quindi nascondere, non solo un testo ma anche un qualsiasi file non TXT.

Enzo Borri



Sono stati presi in esame 16 Pixel di una immagine e viene mostrato il valore dei primi 16 Pixel. Per semplicità, è stata presa una immagine in scala di grigi. Nella parte superiore i dati contenuti nell'immagine originale cui, mediante modifica, sono inserite le lettere "HJ" che hanno rispettivamente i valori "0 1 0 0 1 0 0 0" e "0 1 0 0 1 0 1 0". L'ultimo Bite di ciascun pixel viene così modificato se necessario. Nonostante le modifiche, l'aspetto estetico dell'immagine resta invariato.

COME FUNZIONANO I SISTEMI ANTI CONTRAFFAZIONE DEI PRODOTTI INFORMATICI

PACCO, DOPPIO PACCO

Un sistema operativo a 10 euro? Mouse e tastiera di marca a prezzi bassissimi? O il negoziante si è innamorato di voi, oppure sta cercando di rifilarvi un pacco: un prodotto contraffatto. Ecco come riconoscerli.

La contraffazione è l'imitazione – più o meno esatta – di un prodotto o un oggetto. **Nel mondo informatico si possono trovare programmi contraffatti** al fine di vendere per buoni dei prodotti che sono in realtà dei falsi: manuali, documentazione, copertine del CD… tutto può essere falsificato. Come si può immaginare, **la contraffazione è una forma di pirateria difficile da individuare se ben fatta.**
Visto che i dati copiati sono indistinguibili dagli originali, i produttori di software si tutelano **inserendo nei materiali facenti parte del pacchetto degli elementi "anticontraffazione"**, così chiamati perché difficilmente riproducibili.

>> Immagini olografiche

Si trovano sia su manuali, confezioni dei CD, certificati di autenticità – per esempio Microsoft li usava già al tempo del Dos – e addirittura sugli stessi dischi CD e DVD.
Gli ologrammi rappresentano loghi, marchi o scritte. **Sono di solito realizzati su materiale riflettente di colore argento.** Possono avere anche colori diversi visibili quando la luce viene indirizzata con particolari inclinazioni. Basta prendere un DVD della PlayStation per farsi una idea, e vederli

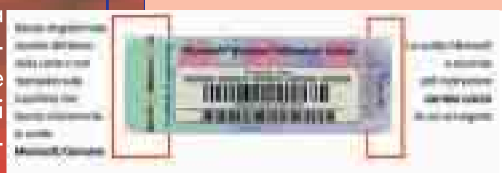


L'ologramma visibile sui CD originali di Windows XP.

sia sulla confezione esterna del supporto dati che addirittura sul lato inciso del DVD. **Si può distinguere un vero da un contraffatto per varie caratteristiche**: la qualità dell'immagine, la differente immagine visibile in funzione dell'inclinazione della luce, sui CD interamente olografati, sulle banconote o sulle carte di credito gli ologrammi sono realizzati direttamente sulla superfice e non sono in genere degli adesivi applicati.

>> Inchiostri speciali

Chi opera nelle arti grafiche ha visto o almeno ha sentito parlare di inchiostri diversi dal comune quali inchiostri termosensibili, fotosensibili, magnetici, visibili agli ultravioletti eccetera. Come sistemi anticontraffazione di solito vengono usati inchiostri termosensibili, magnetici o visibili agli UV.
Gli inchiostri termosensibili reagiscono alla temperatura. Solitamente scaldandoli diventano trasparenti lasciando intravedere per esempio delle scritte oppure cambiano colore. Sono usati anche in altri campi oltre l'anticontraffazione. Per esempio alcune bottiglie di birra hanno stampe a inchiostri termosensibili che **indicano la giusta temperatura per consumare al meglio il prodotto.** Gli stessi inchiostri sono usati per esempio **sui bollini SIAE oltre che sulle copertine o sui Certificati di Autenticità** (C.O.A., Certificate of Authenticity) di programmi.





I certificati di autenticità dei prodotti Microsoft originali hanno delle caratteristiche particolari, che non si incontrano nei certificati contraffatti. Per saperne di più, si può visitare il sito http://www.microsoft.com/italy/softwareoriginale/pid/contraffazione.asp

Gli **inchiostri visibili agli UV** sono usati per realizzare stampe normalmente non visibili ma che appaiono solo se illuminati da una fonte di luce ultraviolet-

CONTROPACCOTTO

ta. Qualche copertina di manuale li usa. Gli **inchiostri magnetici** non sono usati generalmente per l'anticontraffazione di prodotti informatici; sono più spesso usati per le banconote. Si vedono infatti esercenti verificare la autenticità di banconote strisciando su esse un apparecchietto che mostra nella parte a contatto della banconota una testina come quella dei comuni registratori a cassetta. Questa testina infatti trasforma il campo magnetico presente in corrispondenza della stampa con inchiostro magnetico in segnale dati, cosa che permette di verificare l'autenticità della banconota.

>> Strisce nella carta

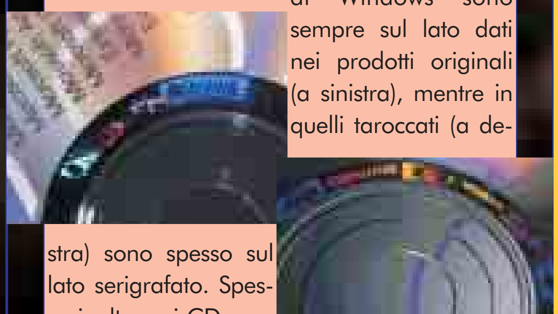
Come si vede spesso nelle banconote, anche nei materiali cartacei dei programmi si possono trovare strisce che si vedono in trasparenza. Le strisce inglobate **sono celate per intero nello spessore della carta, quelle intessute invece sono in parte visibili e in parte sotto lo strato superficiale** della carta. Possono essere semplicemente colorate oppure olografate o stampate con inchiostri termosensibili. **Se sono originali, si nota che nel punto in cui "entrano" nella carta, le fibra della carta sono irregolari**. Se sono delle imitazioni, il passaggio dalla superficie alla carta è solo simulato e si nota un contorno della striscia (nel senso dell'altezza) molto netto. Un esempio dell'uso di questo sistema sono i COA applicati sui computer con sistema operativo in versione OEM.

>> Stampe camuffate

Sono stampe solitamente **coperte da un colore complementare più scuro**. Il sistema era usato anche sulle istruzioni di alcuni giochi onde evitare che venissero fotocopiate. Sono realizzate mediante una stampa, generalmente in azzurro (per la precisione cyan) o in verde chiaro, che rappresenta ciò che dovrà essere letto. In corrispondenza di questa viene stampata con un colore complementare (rosso) un'immagine generalmente molto complessa. **La seconda stampa, quella scura, confonde molto l'occhio umano e non consente la visualizzazione della stampa sottostante** se non usando un filtro di colore adeguato (nel caso in esempio un rosso) in grado di "annullare" la stampa più evidente. Questo sistema rende anche impossibile la fotocopiatura, visto che la stampa sottostante è troppo chiara rispetto a quella di mascheratura.

>> Microscritture

Tipiche di banconote o programmi per cui vi è un rischio concreto di contraffazione, le microscritture sono apparentemente dei ghirigori decorativi o parti di un disegno. **Solo se osservate con un forte ingrandimento si notano delle scritte altrimenti illeggibili**. La ridotta dimensione rende questa tecnica difficilmente riproducibile e difficilmente stampabile con attrezzature comuni. Sono infatti necessarie attrezzature molto precise, pellicole fotografiche in grado di riprodurre fedelmente i dettagli e matrici precise – anche incise tramite laser piuttosto che fotoincise – in grado di garantire una qualità di stampa superiore alle comuni lastre per stampa offset. In fase di stampa occorrono tecniche e inchiostri tali da evitare microsbavature che comprometterebbero la qualità e la leggibilità del risultato finale.



Gli ologrammi presenti nell'anello dei CD di Windows sono sempre sul lato dati nei prodotti originali (a sinistra), mentre in quelli taroccati (a destra) sono spesso sul lato serigrafato. Spesso inoltre nei CD contraffatti le scritte non sono ben leggibili.

>> In conclusione

La conoscenza di questi sistemi potrebbe aiutare a individuare un prodotto contraffatto ma solo a patto di conoscere i sistemi anticontraffazione attuati sull'originale. L'utente finale ha sistemi per tutelarsi molto più semplici: basta acquistare solo da rivenditori accreditati dai produttori o da negozianti di provata serietà professionale.

Enzo Borri

NON FATEVI FREGARE!

• Diffidate sempre dai prezzi troppo concorrenziali: i margini di ricarico sul software sono generalmente bassi ed è difficile per un venditore fare sconti oltre il 5 o 10%.

• Conservate sempre gli scontrini e le fatture: potrebbero dimostrare la buona fede ed evitare una denuncia per "incauto acquisto" o ricettazione nel caso aveste a vostra insaputa acquistato un prodotto contraffatto.

• Non improvvisiamoci Sherlock Holmes: non conoscendo le caratteristiche anticontraffazione dei vari prodotti, è facile credere che il più autentico di questi sia fasullo, o peggio, il contrario!

• Se vi sono dubbi sull'autenticità di un prodotto, conviene rivolgersi sempre e solo al produttore. I sistemi attuati al fine dell'anticontraffazione non vengono generalmente divulgati a negozianti o distributori, e solo i produttori li conoscono a fondo.

TUTTO LO UNIX CHE C'È NEL MACINTOSH

ICONE E TERMINALE

Grazie al suo cuore Unix, su Mac OS X è possibile utilizzare applicazioni fino a ora riservate ai computer col pinguino.

Per molti, Mac OS è sempre stato un sistema poco accessibile a chi voleva smanettarci sopra: solo con programmi per sviluppatori, come ResEdit, si poteva scalfire la superficie di icone colorate. Un po' per questo, un po' per tutti quelle immaginette e suoni simpatici, i veri smanettoni hanno sempre snobbato il Mac, dicendo che **"i veri uomini non hanno bisogno delle icone"**. Ora che tanti terabyte sono passati sotto i router, gli utenti Apple si ritrovano con una macchina dotata di un versatile cuore Unix. Paradossalmente, gli utenti Wintel, tradizionalmente più smanettoni, ora usano un coloratissimo Windows XP, che non ha più una "vera" shell DOS. **Misteri dei corsi e ricorsi dell'informatica...**

>> Mac OS (uni)X

È risaputo che **il cuore di Mac OS X è un sistema Unix**. Per la precisione, si tratta di una particolare versione di BSD 4.4 con parti di FreeBSD 3.2. Probabilmente in tanti hanno provato ad aprire l'applicazione Terminale (in Applicazioni/Utility), a scrivere ls per vedere l'effetto che fa. Se tutto si limitasse a poter dare qualche comando di shell, la novità non sarebbe poi così eclatante. Con **ben poche modifiche, in effetti, moltissimi programmi Unix a linea di comando sono compilabili per Mac OS X.** E se una cosa si può fare, qualcuno che la fa c'è sicuramente: i siti che elencano le nuove applicazioni per Mac sono sempre più affollati di programmi Unix già compilati e pronti da installare. Giusto per fare una lista dei software più conosciuti, per Mac OS X si possono trovare PHP, MySQL, AbiWord, BitchX, nmap, wget, Pine… E i più temerari possono compilarsi i propri a partire dai sorgenti, usando gli strumenti compresi nel CD **Developers Tools, incluso nelle versioni pacchettizzate di Mac OS X e comunque scaricabile gratuitamente** dal sito Apple).



The Gimp eseguito nell'ambiente X11 di Apple. Sulla destra dello schermo si notano i due terminali, quello in ambiente Aqua di Mac OS X (sopra) e XTerm di X11 (sotto).

In effetti le cose non sono proprio così semplici. A complicare le cose, c'è il fatto che il motore grafico Quartz e il gestore di finestre Aqua, non sono compatibili con le applicazioni Unix tradizionali, che utilizzano il sistema Posix. Insomma, **inoltrarsi nel mondo Unix non è proprio una passeggiata per il tipico utente Mac**. Per compilare un programma bisogna impostare correttamente alcune variabili, avere sistemato al loro posto tutte le librerie necessarie, e saperne più di qualcosa sul funzionamento di un sistema Unix. Bisognerebbe fare qualcosa per semplificare tutto il processo…

>> Fink about it

…e qualcosa è stato fatto. Il nome di questo "qualcosa" è Fink, un progetto libero e open source (http://fink.source-

forge.net). Fink agisce come un gestore dei pacchetti software installati. Usando strumenti come dpkg e apt-get presi in prestito da Debian, **Fink permette di gestire una distribuzione software "parallela" all'installazione di Mac OS X**. Una volta avviato, Fink crea infatti sul disco una directory SW, nella quale posizionerà i programmi scaricati, dopo che l'utente li avrà selezionati da una comoda interfaccia. **Fink gestisce automaticamente le dipendenze**: se volete installare per esempio The Gimp, si preoccuperà di scaricare e installare prima XFree86, le librerie gtk e tutto quanto il necessario. Per aggiornare un pacchetto software, basterà dare un comando dal terminale, e Fink farà tutto da solo.
Anche con Fink, però, le cose a volte non vanno come dovrebbero, specialmente quando entrano in campo le applicazioni che hanno bisogno di un server grafico X11. In teoria, selezionando XFree86 tra i pacchetti installabili, Fink dovrebbe "automagicamente" scaricare e configurare tutti i file necessari. In pratica, **raramente questo succede al primo colpo**, tanto che una delle più dettagliate sezioni della documentazione di Fink riguarda proprio la risoluzione di tutti i problemi relativi a X11.

>> X11 per Ten

Tra un ipertrofico PowerBook a 17" e un minimalista 12", durante l'ultima edizione del MacWorld Expo Steve Jobs ha annunciato anche **una versione "ufficiale" del software X11 per Mac OS X**. Si tratta di un annuncio importante, forse più per le sue connotazioni politiche che per i reali contenuti tecnici (anche se difficile da configurare, XFree86 rootless esisteva già). La scelta di creare e supportare una distribuzione di X11 per Mac OS X, **spinge Apple più vicino agli smanettoni orientati verso Unix, e un po' più lontano da Microsoft**. In tanti hanno pensato infatti che la disponibilità di un ambiente X11 per Mac voleva dire soprattutto una cosa: l'imminente rilascio di una versione affidabile di Open Office per Mac, uno dei più validi concorrenti dell'Office di Microsoft in ambiente Linux. Se a questo si aggiunge il fatto che, nella stessa occasione, Jobs ha presentato anche Safari, primo browser marcato Apple dopo CyberDog (del quale siamo in pochi a ricordarci), si ha un quadro piuttosto chiaro dei rapporti sempre più blandi tra Apple e Microsoft.
Con il suo X11, ancora una volta **Apple è riuscita a rendere semplice una cosa difficile**; scaricato il pacchetto autoinstallante, in pochi minuti si è pronti a utilizzare l'ambiente grafico con un semplice doppio clic. A questo punto, scaricare applicazioni grafiche Unix precompilate, installarle e utilizzarle diventa semplice quanto con le tradizionali applicazioni munite di installer. L'unico accorgimento da prendere è quello di inserire nelle preferenze delle applicazioni di X11 la linea di comando necessaria ad avviare l'eseguibile.

>> Linux su Mac

Qualcuno però potrebbe voler desiderare di installare un vero Linux sul proprio Mac. Anche qui, non resterà deluso: se è vero che le distribuzioni Linux per processore PowerPC sono meno aggiornate di quelle per Intel, **ormai hanno raggiunto un grado di maturità che permette loro di essere installate e utilizzate senza grossi problemi**. Tra le distribuzioni più popolari ci sono sicuramente SuSE, Mandrake PPC, Debian e YellowDog, anche se quest'ultima riscuote più successo negli Stati Uniti. Persino chi ha un Mac piuttosto vecchiotto (addirittura con processori precedenti al PowerPC) può trovare distribuzioni adatte al suo computer: una lista completa si trova su www.linux.org/dist selezionando PPC o m68K nel menu Platform.
I vantaggi nell'installare Linux su un Mac sono svariati: **dall'aumento di prestazioni** rispetto al ben più pesante Mac OS X, soprattutto per quanto riguarda l'interfaccia grafica, alla possibilità di avere **un sistema di sviluppo pressoché identico a quello di produzione**, per esempio per chi deve realizzare un sito Web o strumenti di amministrazione. O ancora, per avere a disposizione particolari software che non sono ancora stati portati né su Mac OS X o che non funzionano con il server X11 di Apple.
In definitiva, con tutte le opzioni disponibili, il sistema dei Macintosh non era mai stato tanto aperto e versatile come in questi ultimi tempi.



Volete installare il modulo PHP e MySQL sul vostro iBook e sviluppare siti dinamici anche al mare? Niente di più facile, coi pacchetti precompilati di entropy.ch.

LINK UTILI

www.entropy.ch/software/macosx/
www.tevac.com/entropy-ita/
Sito con i porting per Mac OS X di molti software Unix. Un mirror italiano è su

http://fink.sourceforge.net
Home page di Fink, gestore di pacchetti per Mac OS X.

http://www.apple.com/macosx/x11/
Il server X11 ufficiale di casa Apple.

http://www.linux-mandrake.com/it/ppc.php3
La distribuzione Mandrake è tra le poche per PPC di cui si possano liberamente scaricare le immagini ISO dei CD di installazione.

http://porting.openoffice.org/mac/ooo-osx_downloads.html
Open Office per Macintosh con installati Mac OS X e X11 di Apple.

CONFIGURARE E USARE AL MEGLIO WIN MX PER SCAMBIARE FILE SU INTERNET

2 sistemi in 1

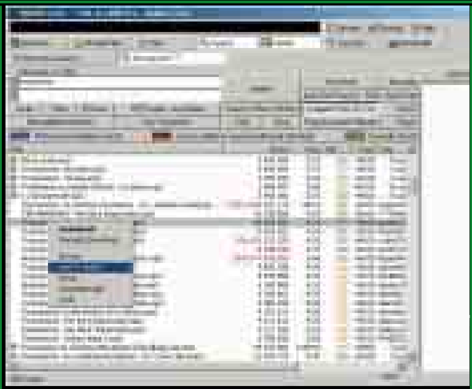


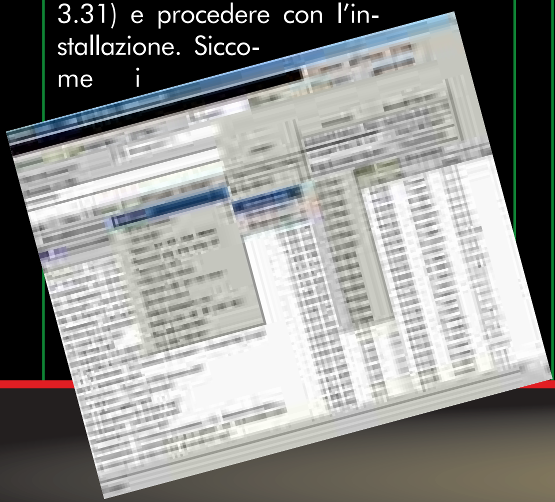
Forse il più usato, sicuramente il più amato, soprattutto dagli utenti italiani. Scopriamo il perché di tanto successo, e come utilizzare al meglio questo diffuso programma di file sharing.

Un client sempre aggiornato, ma con tanti legami col passato (se di passato si può davvero parlare, nella breve storia del peer to peer): forse è questo il segreto di WinMX, che tanta popolarità riscuote fra ai condivisori di file in Rete. Infatti questo programma si basa sulla recentissima rete WPNP, ma è ancora in grado di connettersi ai server OpenNap, più lenti e poco capienti, ma sempre funzionali. Parliamo comunque di una tecnologia senza server centrale, quindi virtualmente non abbattibile o limitabile, e talmente diffusa da poter contare su una rete di utenti (e di file) davvero notevole, con materiale per tutti i gusti.

>> Usare WinMX

Il sito ufficiale è, neanche a dirlo, www.winmx.com. Da lì si può scaricare il client (la versione più recente è la 3.31) e procedere con l'installazione. Siccome i



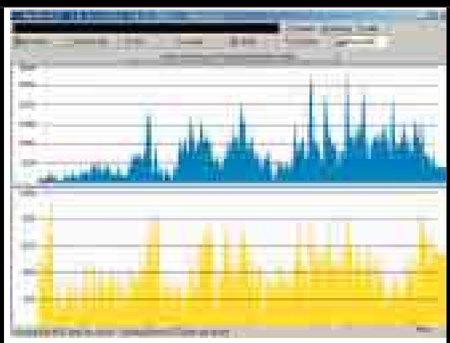


parametri chiesti sono pochi e piuttosto semplici, eviteremo di fare una vera guida all'uso, e ci soffermeremo invece su alcuni aspetti meno conosciuti di questo programma, o su quelli che possono provocare inconvenienti poco piacevoli. Cominciamo subito con la scelta del tipo di nodo. Alla fine dell'installazione infatti possiamo scegliere se effettuare una connessione primaria (se disponiamo di una connessione di alta qualità, che ci fa fungere da server per le ricerche, sacrificando una piccola quantità della nostra banda) o secondaria (per connessioni brevi o di bassa qualità, dialup, reti locali con proxy e firewall e altri casi particolari, che dirotta le ricerche su altre macchine della Rete, ricerche che giocoforza sono più lente che nel caso di una connessione primaria). In ogni caso, se non rispondiamo alle caratteristiche richieste per l'accesso primario, verremo obbligatoriamente dirottati sul secondario.

Da qui possiamo anche scegliere se accedere alla rete WPNP o al circuito OpenNap.

>> Occhi aperti

Forse è inutile ricordarlo, ma non fa mai male. Ogni file scaricato da WinMX deve essere analizzato con un antivirus aggiornato (e per aggiornato si intende aggiornato sul serio, quindi non meno di una settimana/15 giorni prima). In teoria i file Mp3 non comportano rischi di trasmissione virus, sempre che non siano eseguibili camuffati (nel caso non avessimo abilitato la visualizzazione delle estensioni per i file conosciuti). Il controllo invece è tassativo per eseguibili e documenti. Va inoltre prestata attenzione nei confronti di bogus e fake, ovvero file che non sono quello che dicono di essere. Un bogus di solito è un file di dimensioni notevolmente diverse da quelle che ci attendiamo per il file desiderato (verifichiamo quindi sempre questo parametro) mentre per i fake, purtroppo, c'è poco da fare: l'abitudine di rinominare file poco interessanti con nomi più allettanti (film di prima visione o gioco di uscita recente) è tanto diffusa



quanto imprescindibile. I file Mp3 (e anche alcuni file video, a seconda del tipo di codifica) possono essere visti in anteprima durante lo scaricamento: è il solo tipo di controllo possibile. In tutti gli altri casi, non sapremo cosa realmente stiamo scaricando fino alla fine del download. E per questo bisogna fare ulteriore attenzione: potremmo trovarci a visionare, o peggio a far visionare ad altri, materiale non propriamente "pulito", estremamente violento o pornografico. Teniamolo sempre presente. Anche per questo, conviene sempre evitare di utilizzare una stessa cartella sia per i file in arrivo sia per quelli da condividere sulla rete: usando due cartelle diverse potremo "screma-re" il contenuto ed essere sicuri di non distribuire materiale sconveniente o addirittura illegale.

>> Occhio alla banda

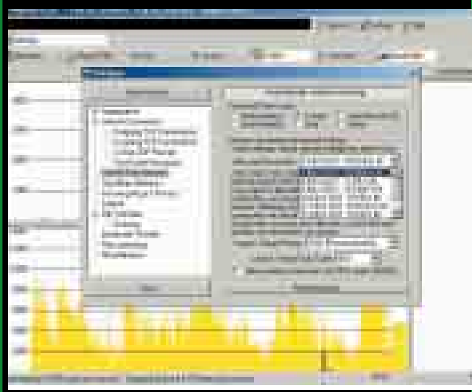
Tutte le connessioni impostate ad alta velocità vengono utilizzate da WinMX come nodi WPNP. Ciò significa che gli altri computer potranno utilizzarci come server di ricerca, con una conseguente (modesta) occupazione della nostra banda a disposizione. È opportuno non disabilitare questa opzione (per rispetto nei confronti della filosofia del peer to peer, che si basa proprio sulla condivisione delle risorse), ma, se stiamo scaricando un file particolarmente impegnativo e abbiamo poco tempo a disposizione, possiamo intervenire su WinMX e disabilitare momentaneamente la funzione di nodo WPNP (Server/Close).



>> Massima potenza

Mxlinx è una utilità reperibile in Rete (www.sharepoint.boo.pl), che aggiunge interessanti funzionalità a WinMX.
Si tenga presente, innanzi tutto, che Mxlinx funziona solo con la versione inglese di WinMX. Detto ciò, prima di installarlo occorre impostare alcuni dettagli in WinMX. Da Settings, si selezioni Any File/Bitrate in Default Search Parameters. Si verifichi quindi di aver abilitato Automatically connect on startup.
Quindi si può procedere all'installazione di Mxlinx, che richiederà la cartella di destinazione dei file scaricati e procederà ad attivare automaticamente WinMX. Fatto ciò, possiamo accedere alle funzioni di generazione dei codici hash e alle modalità antileecher e speedup.Il codice hash è una specie di "firma" di file, una stringa alfanumerica che lo contraddistingue univocamente, differenziandolo da altri con nome simile (o uguale). Attraverso MxLinx si può calcolare automaticamente il codice hash di un file, semplicemente selezionandolo, e quindi recuperarlo a colpo sicuro, facendone il resume. A titolo di cronaca, lo stesso codice può essere recuperato selezionando un file incompleto e facendo clic destro: si tratta del codice alfanumerico che appare nella seconda finestra, preceduto dalla sigla HASH>. O anche isolandolo dal nome del file incompleto, nella cartella dei file scaricati, che è in forma __INCOMPLETE__titolo-autore-codice hash. Questa funzione è utile, in quanto n Rete si possono reperire siti che riportano link diretti ai file mediante il loro codice hash. La modalità antileecher consente di escludere gli utenti "scrocconi", quelli online da più di un'ora senza avere altri utenti in queue o per cui la query Whois non produce risultati. Si attiva con un clic destro su uno degli utenti nella nostra coda d'attesa (a finestra di ricerca Whois chiusa) togliendo il check dalla voce Not only antileecher. La funzione ricercherà e cancellerà dalla coda di attesa tutti gli utenti che non hanno nulla da condividere. La modalità Speedup produce lo stesso effetto della ricerca Search other sources (continua a cercare lo stesso file e lo scarica anche da utenti diversi da quello utilizzato all'inizio), ma la ricerca viene lanciata ogni 5 minuti invece che i 10 di default.

Paola Tigrino



Napigator, alla vecchia maniera

I server OpenNap, sono stati superati dal network WPNP, utilizzato da WinMX fin dalla versione 2.6, potrebbe comunque valere la pena di farci un giro. Per poter accedere alla rete OpenNap mediante WinMX dobbiamo scaricare una utility, Napigator, reperibile presso www.napigator.com, che fornisce a WinMX l'elenco aggiornato dei server.
Dopo aver lanciato Napigator (in modalità standalone) e reperito l'elenco dei server, potremo esportare i risultati in modo da essere leggibili da WinMX, da Server/Export List, salvando in formato compatibile con WinMX (*.wsx). Trasciniamo quindi questo file in WinMX: verrà mostrato l'elenco dei server OpenNap, dai più ai meno "ricchi". I sistemi OpenNap sono particolarmente interessanti per gli utenti di reti a larga banda, come Fastweb; è infatti possibile crearsi un ristretto elenco di server "interni" alla rete metropolitana, che radunano solo altri utenti della stessa rete. Indubbiamente il "catalogo" dei file disponibili sarà molto minore rispetto all'insieme di decine e decine di server, ma si avrà una ragionevole speranza di scaricare a velocità altissime i file trovati. Nel caso di scambio tra utenti Fastweb non è raro toccare punte di 800 Kbyte al secondo.

COME CREARE AREE PROTETTE IN INTERNET INFORMATION SERVER

Cartelle riservate sul Web



Ci sono vari sistemi per proteggere alcune cartelle di un server Web da sguardi indiscreti (ma ancora nessuno che sia davvero a prova di cracker).

Secondo l'autorevole Netcraft, azienda di consulenza informatica che annovera tra i suoi clienti aziende come Microsoft, Sun e IBM, al Dicembre 2002 gli utilizzatori del Web/FTP server di Microsoft (IIS) erano il 28% circa, a fronte del 62% che utilizzano Apache. Sul perché il più famoso server Web abbia raggiunto questi dati e sia in costante crescita da quando è nato è molto semplice dare una risposta: è gratis, è open source, è in media più sicuro dei suoi concorrenti (dico in media perché molto dipende dalla configurazione del sysadmin). Il Web server di Microsoft quindi, nonostante il successo commerciale di Windows 2000 Server, con cui IIS 5.0 viene dato in bundle, non riesce ancora a convincere la maggior parte dei sysadmin che, nonostante abbiano magari acquistato una dispendiosa licenza Microsoft, vi installano su Apache. Il punto dolente è evidentemente la sicurezza. Vediamo come la casa di Redmond ha fronteggiato la situazione nell'ultima versione del suo bistrattato Web server: in particolare vedremo in dettaglio che possibilità da IIS 5.0 a chi vuole creare sul proprio server Web aree protette da autenticazione. Qui daremo principalmente una carrellata ai vari sistemi. Per evitare di esagerare con le dimensioni dell'articolo devo rimandarvi per i dettagli sull'implementazione dei vari metodi al seguente indirizzo: http://www.microsoft.com/technet/prodtechnol/iis/maintain/featusability/authmeth.asp

>> Autenticazione anonima

Cito questo tipo d'autenticazione soltanto per completezza. Essa viene applicata alle parti pubbliche del server Web. All'utente che entra in una qualunque pagina vengono attribuiti dal sistema i criteri di protezione relativi all'utente IUSR_nomecomputer senza che naturalmente avvenga alcuna richiesta di nome utente e password. Di default IUSR_nomecomputer appartiene al gruppo Guest per limitarne le possibilità. Qualora si vogliano creare altri utenti anonimi, è opportuno naturalmente copiarne gli attributi. Per implementare questo tipo d'autenticazione è

sufficiente selezionare anonymous access nelle proprietà del sito o della directory virtuale che ci interessa. Inoltre bisogna fare in modo che le parti pubbliche del sito abbiano accesso ad Everyone in lettura (vedi figura 1).



Figura 1. Le parti pubbliche del sito devono essere impostate su Everyone.

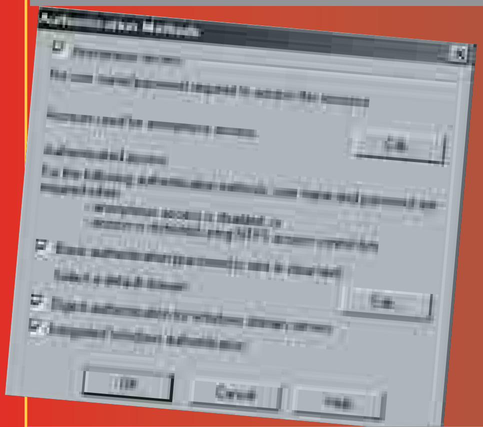


Figura 2. La finestra da cui si impostano i metodi di autenticazione per una risorsa.

>> Autenticazione di base

L'autenticazione di base è probabilmente quel tipo d'accesso che vi sarete trovati di fronte centinaia di volte. Come funziona? Quando il browser riceve dal server la richiesta di credenziali per la visualizzazione di risorse protette, il browser visualizza sul computer dell'utente la classica finestra con nome utente e password (figura 3), a questo punto l'utente può inserire i suoi dati (il nome utente può anche essere introdotto nella forma dominio\nomeutente). In caso di dati non corretti viene rivisualizzata la finestra di logon. In questo tipo d'autenticazione i dati vengono inviati dal browser al server semplicemente codificati in Base64 e quindi non cifrati; conseguenza di ciò è che un eventuale soggetto "in ascolto" potrebbe carpirli. Per far fronte a questo proble-



Figura 3. Modulo per l'autenticazione di rete.

SSL Secure Sockets Layer, un protocollo sviluppato da Netscape per cifrare i dati in transito tra il server e il browser Web.

ma è possibile integrare IIS con i protocolli cifrati SSL/TLS. Nel qual caso è necessario dotare il server di un certificato con la relativa chiave privata ottenuto attraverso un'Autorità di Certificazione nota. In caso di certificato proprietario, è necessario distribuirlo preventivamente ai browser dei propri utenti come avviene per alcune banche per l'attivazione dell'home banking. Il vantaggio principale dell'autenticazione di base è la sua appartenenza agli standard del protocollo http e quindi la sua compatibilità con tutti i browser internet. Per implementare questo tipo d'autenticazione è necessario impostare degli account sul server con accesso in locale ed impostare sulle risorse del Web i diritti d'accesso relativi ad ogni utente.

>> Autenticazione classificata

Ovvero Digest Access Authentication. Questa autenticazione è del tipo Challenge/Response (come l'NTLM per intenderci). Essa è descritta nel dettaglio nell'RFC 2069 dell'IETF (Internet Engineering Task Force) reperibile al seguente indirizzo http://www.ietf.org/rfc/rfc2069.txt?number=2069. Il modo in cui opera questo tipo d'autenticazione è il seguente:
Il server invia al browser il cosiddetto Challenge costituito da alcune informazioni di verifica quali l'identità del computer client, il dominio in cui avviene l'autenticazione e l'ora.
Questo per evitare che qualcuno possa riutilizzare la risposta. Il browser richiede all'utente l'inserimento di nome utente e password come per l'autenticazione di base. Il browser sul client a sua volta effettua l'hashing della password e del Challenge insieme ed invia il risultato al server. Per hashing si intende applicare una funzione di hash (come l'MD5) a una stringa.
Generalmente una funzione di hash riceve in ingresso una stringa di qualunque dimensione e genera una stringa di dimensione fissa che dipende in modo univoco dalla stringa in ingresso. Viene assiduamente utilizzata nella crittografia perché facilita il confronto tra due stringhe riducendolo al confronto tra due hash.
Il server effettua la stessa operazione ossia esegue l'hashing del Challenge e della password relativa al nome utente e lo confronta con l'hash ricevuto dal browser.
Se i due hash coincidono concede l'accesso alle risorse.
L'autenticazione classificata è stata introdotta nello standard http con la versione 1.1 perciò la supportano esclusivamente i browser che si riferiscono a quello standard (praticamente, qualsiasi browser attualmente utilizzato). Qualora ci si colleghi con un browser non valido può non essere restituito un messaggio d'errore ed il browser potrebbe continuare a richiedere l'autenticazione. Requisito fondamentale per questo tipo d'autenticazione è che gli utenti siano definiti come utenti del dominio e che quindi abbiano l'accesso alla rete, questo perché la Digest Authentication si applica ai domini e non a server stand alone. Segnalo inoltre che essa funziona anche attraverso proxy o firewall.

COME CREARE AREE PROTETTE IN INTERNET INFORMATION SERVER

Autenticazione integrata di Windows

IIS permette di applicare al Web le stesse procedure d'autenticazione che vengono utilizzate da Windows 2000 per il normale accesso in rete ossia NTLM e Kerberos. Sui dettagli di questi tipi d'autenticazione abbiamo già detto in numeri precedenti di HJ. Qui mi interessa descrivere soltanto cosa avviene tra browser e server. Premetto che il browser cui mi riferisco è Internet Explorer, che naturalmente è l'unico a supportare l'autenticazione integrata.
Nel momento in cui si cerca di accedere a una risorsa, e qualora l'utente sia già loggato nella rete, Internet Explorer tenta di utilizzare le credenziali registrate.
Se il tentativo non ha esito favorevole, perché l'utente non si è loggato nel dominio oppure è loggato presso un dominio diverso, allora Internet Explorer visualizza la classica finestrella d'autenticazione.
È necessario però puntualizzare alcune cose che rendono poco utilizzabile questa procedura: innanzi tutto, come abbiamo già detto, funziona soltanto con IE dalla versione 2.0 in poi per quanto riguarda l'autenticazione NTLM, mentre per Kerberos ci vuole almeno il 5.0. Inoltre i client devono appartenere a un dominio Windows 2000. Per tutte queste ragioni è conveniente utilizzare questo tipo d'autenticazione soltanto nelle reti intranet.

Autenticazione con ASP

Se le risorse da proteggere sono costituite da pagine Web, un'alternativa valida a queste autenticazioni è l'utilizzo di Active Server Pages, possibilmente utilizzando un database che si trovi al di fuori di \wwwroot, attraverso un DSN. Questo consente di evitare di creare troppi account sul server qualora gli utenti da configurare siano molti, riducendo quindi le probabilità di un attacco a forza bruta.

Le modalità di autenticazione che adesso vedremo non sono sicure al 100%, ma possono essere utili a chi volesse inserire un'area protetta sul proprio sito personale o cose del genere.

> **DSN** Data Source Name. Un sistema che permette di collegarsi a un database a partire dal nome con cui è stato registrato, e senza accedere direttamente al file, che quindi può trovarsi in qualsiasi posizione sicura del server.

Partiamo innanzi tutto dal form che bisogna creare nella eventuale pagina di login:

```
<form method="POST" action=
            "pagina_da_proteggere.asp">
  <p align="center">Username
                  <input type="text"
       name="username" size="20"><br>
  Password <input type="password"
       name="password" size="20"></p>
  <p align="center"><input
         type="submit" value="Log in"
                   name="log_in"></p>
</form>
```

A questo punto presentiamo due possibilità:
a) Utilizzare uno script più semplice che però consente l'utilizzo di un unico nome utente ed una password per la protezione dell'area senza l'utilizzo di un database;
b) Utilizzare uno script ugualmente semplice ma con un collegamento ad un database.
Per implementare la prima soluzione basta aggiungere alla pagina_da_proteggere.asp il seguente script prima di qualunque istruzione html:

```
<%
  If  Replace(request.form("userna-
me"),"'","''") <> "nomeutentescelto"
AND _
        Replace(request.form("pas-
sword"),"'","''") <> "passwordsscel-
ta" THEN
      Response.Redirect "login.htm"
  End if
%>
```

Potete poi sostituire nomeutentescelto e passwordscelta con i vostri dati di autenticazione. In realtà potreste aggiungere altri account semplicemente ampliando l'If con delle istruzioni OR però, anche se lo script funzionerebbe ugualmente, non sarebbe proprio il massimo della funzionalità e dello stile.
La seconda soluzione sfrutta la presenza di un database in Access che si trova all'interno del nostro sito nella cartella \db. All'interno del database deve essere creata una tabella chiamata T_utenti che abbia tre campi: uno di nome ID come campo contatore, un campo che si chiama username ed un campo password, entrambi definiti come campi testo. Questa volta le pagine da utilizzare sono tre: la pagina di login (login.htm) su cui va sempre il form di sopra, la pagina da proteggere ed una pagina di autenticazione che chiameremo autentica_utente.asp. Ecco la pagina autentica_utente.asp che deve essere richiamata dall'action del form nella pagina login.htm:

```
<%
  dim conn
  dim strconn
  strconn = "DRIVER=Microsoft Access
Driver (*.mdb);DBQ=" & _
         Server.MapPath("/db/uten-
ti.mdb") 'path del database
  set              conn           =
server.createobject("adodb.connec-
tion")
  conn.open strconn
  Username                        =
Replace(Request("Username"),   "'",
"''")
  Password                        =
Replace(Request("Password"),   "'",
"''")
  SQL  =  "SELECT  *  FROM  T_utenti
WHERE username = '" & username & "'"
& _
        "AND password ='" & password
& "'"
  set oRs = conn.Execute(SQL)
  If oRs.EOF then
    Response.Redirect("login.htm")
  Else
    session("ID")    =    "sessione"
'sostituibile con qualunque parola
  End If
  Set conn = Nothing
  Set oRs = Nothing
%>
```

All'inizio della pagina da proteggere inserite il seguente script:

```
<%
  If  session("ID")  <>  "sessione"
THEN
    Response.Redirect "login.htm"
  End if
%>
```

Il funzionamento di questa procedura è il seguente: la pagina autentica_utente.asp confronta i dati inseriti nella pagina di login con quelli presenti nel database attraverso una query SQL; se il confronto non va a buon fine, l'utente viene rimandato alla pagina login.htm, altrimenti viene creato un id di sessione con il nome 'sessione' (sostituibile con un qualunque nome). Quando un utente a questo punto accede ad altre pagine della zona protetta che hanno all'inizio lo script di protezione, la pagina effettua un controllo sul nome sessione e nega/consente l'accesso all'utente.

Roberto "dec0der" Enea

MID HACKING

TECNOLOGIA ALLA BASE DELLE RETI DI COMUNICAZIONE



Dal cavo al browser

Prima di addentrarci in qualche scorribanda digitale, occorre conoscere bene il funzionamento delle reti.

Nel momento in cui andiamo a parlare di reti di comunicazione possiamo farlo affrontando l'argomento da due punti di vista: quello dei **dispositivi**, e quello dei **protocolli**.
Come è ovvio i due aspetti sono fortemente legati l'uno all'altro, dato che il primo descrive la natura fisica delle interconnessioni fra PC con un occhio di riguardo alle schede, ai cavi e a ogni altro supporto materiale, mentre il secondo disegna i metodi di interconnessione e di comunicazione adottati. **L'implementazione** dei due protocolli è il momento dell'unione fisica dei due aspetti in questione.
Tralasciando momentaneamente il primo punto, passiamo ad analizzare i protocolli e le loro funzionalità.

Peer to peer: connessione diretta fra due host.

>> Una questione di protocollo

Genericamente **si definisce protocollo la struttura dei dati che vengono scambiati e le modalità utilizzate per lo scambio**. Un fatto che però non è specificato è l'interazione che un protocollo ha con altri protocolli di livelli superiori e inferiori, prendendo funzioni complesse dai primi e dando le proprie ai secondi. **La struttura gerarchica che si viene quindi a realizzare è quella classica fatta a strati**, dove ogni strato utilizza le potenzialità dello strato sottostante per realizzarne di nuove in favore di quello superiore.
Nel nostro caso, il punto cardinale su cui gira tutto è la **comunicazione**. Ciò che uno strato fa rispetto all'inferiore e al superiore altro non è se non "maneggiare" e articolare una certa comunicazione. **L'interfaccia di comunicazione** è l'insieme della funzionalità che uno strato è in grado di offrire. Le comunicazioni che avvengono tra agenti dello stesso strato sono



Se oggi facciamo con Internet tutto ciò che sappiamo, dobbiamo dire grazie a questi "ragazzi".

dette **peer-to-peer** e utilizzano un protocollo comune, chiamato anche linguaggio, che comprende sia la struttura sia le modalità con cui avviene lo scambio. Ma cos'è in pratica che viene scambiato nel momento in cui si sia instaurata una comunicazione? Viene scambiato **quello che tecnicamente è denominato protocol data unit (PDU)**, il quale è composto essenzialmente da due parti:

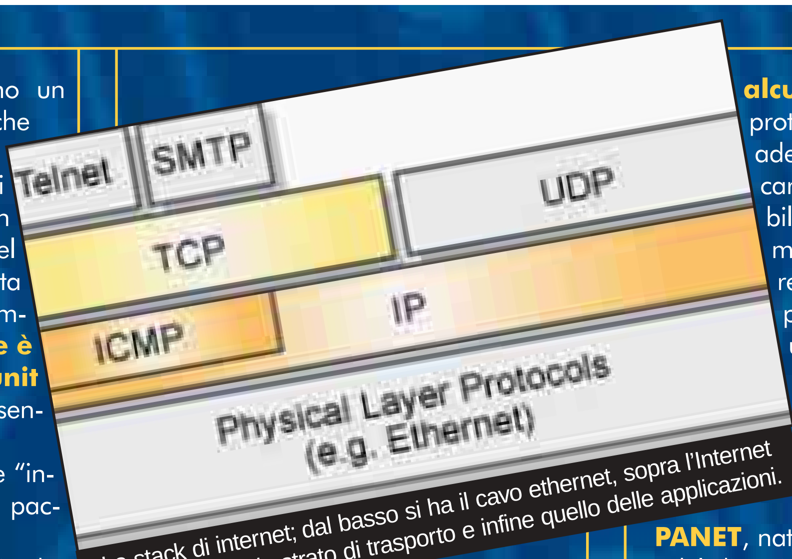
- **Header**: che contiene le "informazioni di viaggio" per quel pacchetto
- **Payload**: che contiene ciò che noi effettivamente vogliamo mandare al destinatario.

> **?** **PDU:** protocol data unit, è l'insieme dei dati che viene scambiato durante una comunicazione ed è formato dall'header e dal payload.

In pratica il primo è la parte attiva del protocollo, e contiene tutte le informazioni sul mittente, sul destinatario, sull'ordine di ricostruzione dei pacchetti e così via, mentre il secondo è il carico utile, ovvero ciò che dobbiamo spedire e che non entra mai nelle manipolazioni del protocollo.

Tutti gli strati hanno regole proprie di manipolazione dell'header, fra le quali è utile ricordare:

- **Connessione e sconnessione**: modalità con cui esse avvengono.

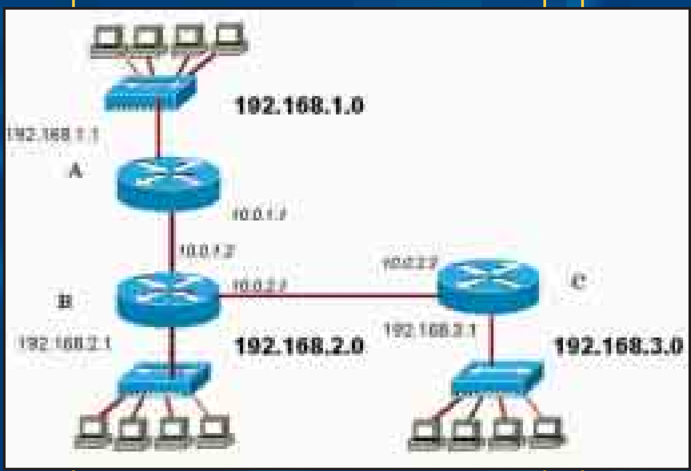


Lo stack di internet; dal basso si ha il cavo ethernet, sopra l'Internet Protocol, sopra lo strato di trasporto e infine quello delle applicazioni.

- **Trasferimento dati**: tempi e modalità di effettuazione.
- **Controllo del flusso**: serve per sincronizzare mittente e destinatario.
- **Controllo errori**: gestisce le situazioni particolari cercando di porvi rimedio.
- **Frammentazione**: divisione del payload in base alle massime possibilità di ogni singolo protocollo.

> **?** **Multiplexing / demultiplexing:** interfaccia condivisa da più di un agente dello strato superiore.

- **Ricostruzione**: riassemblaggio del payload.
- **Multiplexing e demultiplexing**: realizzano interfacce condivise fra più agenti dello strato immediatamente superiore.
- **Routing**: capacità di individuare la strada meno "dispendiosa" fra due punti.



Il routing è quel processo per cui alcuni nodi sono deputati alla ricerca della "strada migliore" fra le varie parti della rete.

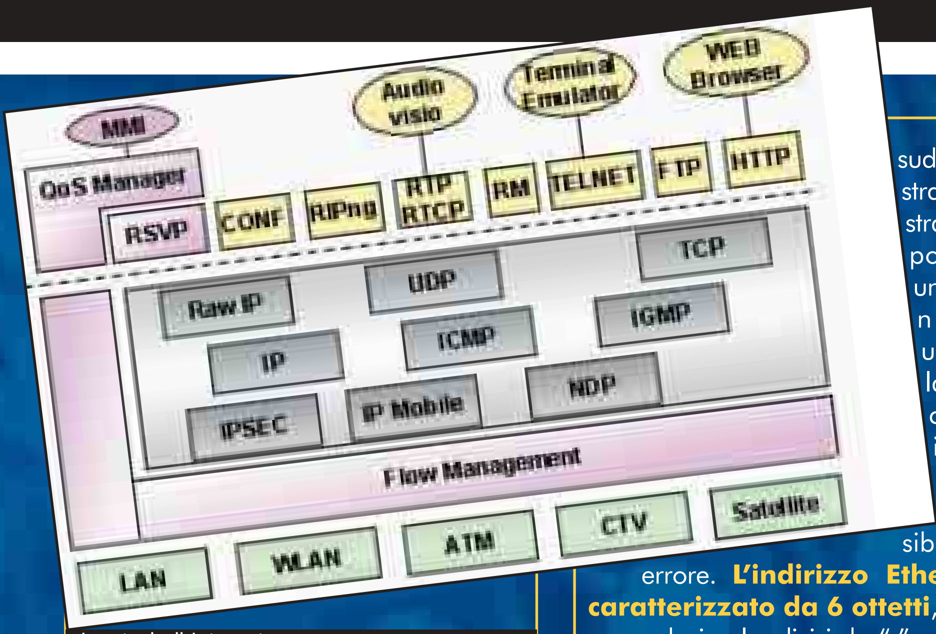
>> I modelli canonici

Data la mole delle decisioni che devono essere adottate singolarmente da ogni strato, si rende necessaria una **politica di standardizzazione che tenda a rendere fisse alcune regole** a cui ogni protocollo alla fine si deve adeguare per poter comunicare in maniera "comprensibile" con tutti gli altri. Il primo standard applicato alle rete fu l'OSI, accantonato però ben presto a causa di una serie di punti difficilmente applicabili nella pratica. Mentre OSI perdeva sempre più di popolarità, **di pari passo cresceva invece ARPANET**, nata nel 1969 da un progetto del dipartimento di difesa degli stati uniti, ed assimilabile ad OSI per un parametro fondamentale, ovvero la stratificazione gerarchica.

La differenza fondamentale risiede però nel numero di strati presenti. Mentre **in OSI sono presenti ben sette strati**, con tutti gli inconvenienti che può portare la necessità di dover attraversare un numero così alto di stazioni computazionali, in ARPANET essi **sono ridotti a tre**, che pur svolgendo le stesse funzioni riducono il numero di errori possibili.

Il primo strato di ARPANET è quello di interconnessione fra reti, individuato nel protocollo IP. Questo è possibile in quanto, a differenza di OSI che vedeva la rete come unica e non strutturata, ARPANET definisce una rete come un insieme di **interconnessioni tra reti più piccole basate su un protocollo connectionless (senza connessione costante)**. Il secondo strato è caratterizzato dai protocolli di trasporto; sono due in ARPANET, uno connectionless ed uno connection oriented, chiamati rispettivamente **UDP e TCP**. Come ultimo strato abbiamo quello delle applicazioni (sessione, presentazione e applicazione nello standard OSI).

> **?** **Routing:** funzione che cerca la strada migliore fra due punti di una rete.



Lo stack di Internet.

>> ARPANET, ovvero: Internet

Ma in pratica…come funziona realmente?? Vediamo di dare uno sguardo all'anatomia e alla fisiologia di un nodo Internet, cercando di capire come funzionano i vari **moduli** e come sia organizzato lo **stack** del protocollo.

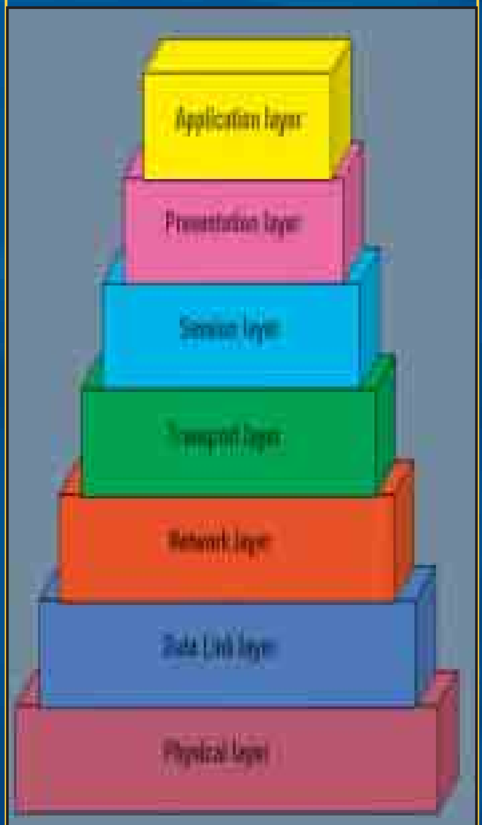
> **UDP — TCP:** sono le due varianti dello strato di trasporto; il primo connectionless, il secondo connection oriented.

Al di sopra del cavo ethernet (maledetta tecnologia: ora ci sono anche le connessioni wireless per farmi ammattire…ma per ora consideriamo il cavo) si trova un **transreceiver Ethernet** che è il dispositivo in grado di trasferire i dati al PC. Immediatamente superiore a esso si trova il **driver** che è un programma che comunica con l'hardware del PC.

In Internet, il dato fondamentale è l'ottetto, che altro non è se non **una sequenza di otto bit in grado quindi di realizzare 256 valori differenti**. Come abbiamo detto, il nodo è suddiviso in strati e ogni strato deve possedere un proprio nome, unico nella rete, che lo identifichi senza possibilità di errore. **L'indirizzo Ethernet è caratterizzato da 6 ottetti**, di natura esadecimale, divisi da ":"; un esempio potrebbe essere A2:C3:F2:Q1:S2:T1.

> **Arpanet:** rete nata nel 1969 presso il dipartimento di difesa americano. Sarà la base di internet.

Diversamente, **l'indirizzo IP del computer è formato da 4 ottetti** che lo identificano in maniera unica all'interno della rete. L'IP è rappresentato come una serie di quattro numeri in base 10, compresi fra 0 e 255 e separati da ".". Infine c'è la **porta, rappresentata da due ottetti**, come un numero compreso fra 0 e 65535 che identifica in maniera inequivocabile un servizio all'interno di quel nodo.



Nella figura si possono notare i sette strati del modello OSI. Ricordiamo che Arpanet ne prevede solo tre.

Ogni strato quindi può ricevere messaggi da due direzioni: quella superiore e quella inferiore, e si comporta come interfaccia verso la rete per lo strato superiore, utilizzando quella dello strato direttamente sottostante.

In pratica un'applicazione generica userà nell'ordine: applicazione, UDP o TCP, IP, driver per accesso Ethernet.

>> Multiplexing e demultiplexing

Come detto, nello strato di trasporto trovano posto i moduli TCP e UDP. Essi si possono comportare come multiplexer o come demultiplexer, rispettivamente se il pacchetto viaggia verso il basso o verso l'alto. Anche il modulo IP può comportarsi in entrambe le maniere. Questo è facile da intuire se per esempio un nodo ha due connessioni Ethernet su due reti diverse; IP si comporterà da demultiplexer inviando verso lo strato TCP/UDP un frame proveniente da Ethernet, mentre agirà da multiplexer riversando su Ethernet un datagramma o un segmento proveniente dall'alto.Esiste infine un ultimo tipo di applicazione dell'IP chiamato **IP forwarding**, in cui tutti i frames che arrivano non vengono mai inoltrati verso l'alto ma rediretti tutti verso un'altra rete. Come avrete ben capito è questa la base del **routing**.

> **OSI:** Open System Interconnection. Primo tentativo di standardizzare la comunicazione internet (1984), tuttora valido come modello di insegnamento ma poco applicato nella realtà.

Nel prossimo numero analizzeremo più in dettaglio il protocollo TCP/IP, e vedrete come tutta questa teoria possa essere messa in pratica.

CAT4R4TTA,
cat4r4tta@hackerjournal.it

UN PROGRAMMA PER SFRUTTARE I PROXY IN VISUAL BASIC

Anonimizziamoci!



Ogni volta che il nostro computer si collega a un server, lascia le sue "impronte digitali" nei log di accesso. A meno di non utilizzare un proxy; vediamo come costruire un programma che semplifica molto le cose...

Alzino la mano quelli di voi che hanno usato almeno una volta un programma per navigare anonimi? Se potessi vedervi, certamente le mani alzate sarebbero un buon 90%. Qualunque sia il sistema di navigazione anonima da voi sfruttato (Anonimizer, Multiproxy, etc....), **tutti quanti si basano sull'utilizzo di un server proxy**.
In questo articolo vedremo come costruirci un programma tutto nostro per la navigazione anonima che sfrutti tale tecnica; prima però vediamo di chiarire un pochino l'idea su cosa serva il sopraccitato proxy.

>> Come funziona un proxy

Durante una normale sessione Internet, quando con il nostro browser vogliamo visualizzare una pagina html, non facciamo altro se non collegarci alla porta numero 80 di un server. Ovviamente, **il sito vedrà giungere la richiesta direttamente dal nostro indirizzo IP** e la soddisferà inviandoci la pagina. La richiesta che il sito si vedrà arrivare sarà del tipo:

GET www.sito.it/ HTTP/1.1
In questo caso, non essendo specificato direttamente il nome del file che vogliamo (*.html, *.asp, *.pl, etc....) il server ci invierà il file index.html , ma nulla ci vieta di indicare anche il nome di ciò che desideriamo visualizzare.
Ora però entra in gioco il proxy.
Il GET non deve necessariamente essere inviato al sito target, ma possiamo appoggiarci ad un server proxy, il quale soddisferà le nostre richieste **rigirandole al sito-obiettivo**. Quest'ultimo **vedrà arrivare la domanda dall'IP del proxy, e non dal nostro**. Se il server proxy non tiene traccia del nostro IP, ma si dimentica di noi una

volta che ha portato a termine il suo compito, ecco che abbiamo ottenuto il nostro scopo: **abbiamo navigato in modo anonimo**.
In rete basta formulare ad un qualunque motore di ricerca la query "proxy + anonimo + lista" per ottenere alcuni indirizzi dei famigerati (ma quanto mai utili) proxy-anonimi presenti in giro per il mondo; **è importante che vi annotiate anche la porta su cui connettersi al fine di poter utilizzare il servizio** (generalmente: 80, 8080, 8088).

>> Chiarimenti su multiproxy

In un precedente articolo apparso su HJ si è parlato di Multiproxy, un programma simile a quello che andremo a realizzare. **Su tale software, si è creata un po' di confusione**, infatti molti credono che indicando nella sua proxylist più di un server, questo attraversi contemporaneamente tutti quelli abilitati prima di raggiungere il sito target. Sbagliato! Se proviamo a costruirci un paio di serverini e a indicare questi al Multiproxy come IP validi, noteremo come il programma usi a rotazione tali nostri server, ma **sempre e solo uno alla volta**. E se per caso ci siamo sbagliati e uno dei proxy ha loggato le nostre attività? **Addio anonimato.**
Ecco perché è bene essere certi che tutti i server indicati a Multiproxy siano effettivamente anonimi!
Inutile dire che anche se ci colleghiamo ad uno di quei servizi che ci fa vedere il nostro presunto IP, così da poter valutare quanto siamo "anonimi", in realtà non possiamo sapere se non rimarrà traccia alcuna della nostra visita: magari non siamo visibili ad un traceroute (il metodo solitamente utilizzato per dimostrare il nostro anonimato) direttamente al sito, ma **è comunque possibile risalire a noi tramite il proxy**. Nessuno infatti ci garantisce che il gestore del proxy non consulti i suoi log, e li fornisca a chiccehssia, mandando a ramengo la nostra anonimità e la nostra privacy.

>> Programmiamo

Innanzitutto vediamo cosa ci serve: Visual Basic 6.0.
Cominciate con l'aprirvi un nuovo progetto standardEXE e una volta che vi ritrovate davanti la classica form vuota, cliccate sulla barra dei menu **Progetto->Componenti**. Se avete fatto tutto bene vi apparirà una schermata con una lista dei controlli da poter includere nel proprio progetto: selezionate il Winsock e il RichTextBox e basta.
Ora inserite nella form i seguenti controlli:

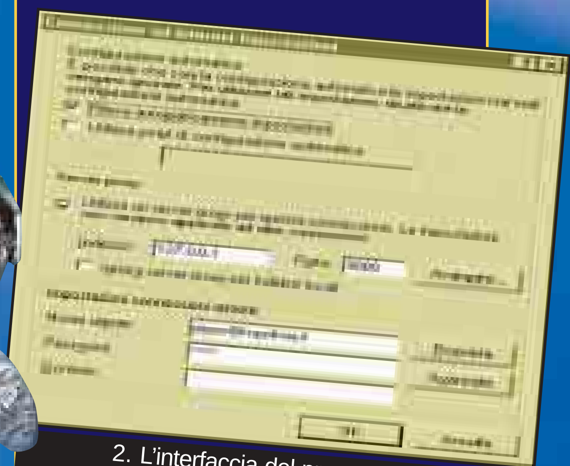
CONTROLLO	PROPRIETA'	VALORE
Text1	Multiline	True
Text2	MaxLength	4
Text3		
Command2	Caption	Chiudi
Label1	Caption	Proxy
Label2	Caption	Porta
Label3	Caption	Sconnesso
Winsock1	Local	Port 8080
Winsock2		
RichTextBox1		
Timer1	Interval	10

Otterrete un risultato simile a quello mostrato nella figura 1.



1. L'ambiente di sviluppo di Visual Basic, con tutti gli elementi disposti.

Bene. Ora bisogna inserire il codice indicato nel riquadro in queste pagine. Se siete pigri, lo potete trovare online all'indirizzo: www.hackerjournal.it/codici/19
Prima di studiarlo assieme apriamo il nostro browser preferito e impostiamo le connessioni affinchè utilizzino il proxy sull'indirizzo 127.0.0.1 (il nostro) e la porta 8080. In questo modo, abbiamo istruito il browser per non collegarsi direttamente al server richiesto, ma di passare attraverso il proxy locale, che a sua volta lo indirizzerà verso un proxy esterno.



2. L'interfaccia del programma realizzato.

>> Analizziamo il codice

Quando il browser vorrà collegarsi ad un sito, **invierà la richiesta al nostro programma**, il quale essendo in ascolto sulla porta 8080 la riceverà e si preoccuperà di girarla sulla porta del server proxy indicata da noi nella due textbox centrali.
A questo punto **il nostro anonimizzatore riceve la risposta dal sito e la manda al browser**. Terminata questa fase si chiudono tutte le connessioni attive e il nostro software rimane ancora in ascolto pronto ad esaudire i nostri futuri desideri.
Per realizzare quanto appena detto, il nostro programma utilizza due controlli Winsock distinti. Il primo, grazie al metodo Listen, **rimane in ascolto sulla porta LocalPort da noi inizializzata sul valore 8080**. Grazie alla funzione ConnectionRequest, quando riceve una richiesta di connessione, la accetta tramite Accept. A questo punto rimane in attesa di eventuali dati, che quando il browser invierà attiveranno il metodo DataArrival; Winsock1 si preoccuperà di leggere i dati, di visua-

UN PROGRAMMA PER SFRUTTARE I PROXY IN VISUAL BASIC

lizzarli sulla casella di testo inferiore (text1) e di avvisare Winsock2 che può iniziare a lavorare.
Ora **Winsock2 cerca di connettersi tramite il metodo Connect sulla porta RemotePort di RemoteHost**. Tali valori vengono presi da text2 e text3, e se la connessione viene accettata dal server, allora si attiva la funzione Winsock2_Connect. Così facendo si rigira la richiesta (quella che possiamo vedere su text1) al proxy e Winsock2 rimane in attesa di ricevere una risposta. Giunta la risposta del proxy, Winsock2 la scarica tramite il metodo GetData e, visualizzata sulla RichTextBox1, la passa a Winsock1, il quale la spedisce al browser. Terminato l'invio, Winsock1_SendComplete si preoccuperà di chiudere le connessioni dei due winsock e di rimettere il numero uno di nuovo in ascolto.
I pù' attenti di voi avranno notato anche un timer; l'ho inserito per far sì che aggiorni ogni 10ms la label1indicandoci lo stato della connessione.
I DoEvents sparsi qua e là servono a non saturare le risorse della nostra macchina mentre il software lavora.

>> Migliorie

Tra le possibili migliorie si potrebbe **aumentare il numero dei proxy** e utilizzando un qualunque criterio di scelta, selezionarne uno alla volta. Multiproxy docet!
Altra cosa possibile è **migliorare il controllo sui dati che il server ci invia**: normalmente la richiesta del browser non supera le 15 righe, sicché è possibile memorizzarla tranquillamente su una stringa, ma il proxy potrebbe risponderci con un quantitativo di dati enorme (perché magari ci passa anche moltissime immagini o un video), difficilmente gestibili senza una seria verifica del buffer.
Altro limite del programma è il poter soddisfare **al massimo una richiesta**. Aumentando in maniera intelligente il numero delle connessioni sarebbe possibile gestire più browser aperti. Non aggiungete però solo dei controlli winsock sul form; già cinque, infatti, appesantiscono molto le richieste hardware



del programma: esistono altri metodi più "da programmatore", che comunque lascio a voi per esercizio.

>> Conclusioni

Alcuni di quei servizi, menzionati sopra, che visualizzano su di una pagina html il "nostro" IP, consentendoci di valutare se siamo nascosti o meno, **potrebbero riuscire a mostrare il vostro vero indirizzo**. Molto probabilmente usano ActiveX, Applet o JScript. Tramite alcune delle tecnologie indicate, **inducono il browser ad aggiungere nella richiesta della prossima pagina da visualizzare, l'IP che abbiamo**. Così facendo, il browser ci smaschera.Il famoso GET può infatti essere corredato da altre indicazioni, quali il tipo di browser stesso, se vogliamo o meno scaricare le immagini collegate alla pagina, la lingua che preferiamo, il nostro username, l'IP...

E la navigazione anonima dove sta?

Non c'è piu!.
Ricordo che le Applet sono codice java eseguito dal client (noi), e se questo riempisse a nostra insaputa con il nostro IP ad esempio un controllo HIDDEN presente su di un form contenente solo questo campo (così da risultare invisibile ai nostri occhi), saremmo visibili senza saperlo.
Successivamente, quando crederemo di cliccare su di un innocuo link, questo magari tramite javascript invia il valore del form con method="get".
Così facendo noi ci stiamo "sputtanando" da soli! Io ho realizzato una pagina come quello appena spiegato, e credetemi non potreste nascondervi... A dire il vero un sistema c'è: **disabilitate Java e Javascript durante le scorribande anonime**.

loxeo@hackerjournal.it

Il listato dell'anonimizzatore



```
Private Sub Command2_Click()
    'Chiudo prematuramente e forzatamente
    'la connessione
    On Error Resume Next
    Winsock1.Close
    Winsock1.Listen
    Winsock2.Close
    Label1.Caption = "SCONNESSO"
End Sub

Private Sub Form_Load()
    'Appena apro il programma mi metto in ascolto
    Winsock1.Listen
End Sub

Private Sub Timer1_Timer()
    'Verifico lo stato della connessione
    'e lo visualizzo
    If Winsock1.State <> sckConnected Then
        Label1.Caption = "SCONNESSO"
    Else
        Label1.Caption = "Connesso"
    End If
End Sub

Private Sub Winsock1_ConnectionRequest
                                (ByVal requestID As Long)
    'Quando giunge una richiesta l'accetto
    If Winsock1.State <> sckClosed Then
                                          Winsock1.Close
    Winsock1.Accept (requestID)
    Label1.Caption = "Connesso"
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As
                                                   Long)
    'Il browser ha formulato la richiesta: inizia a
                                                lavorare
    Dim buffer As String
    Winsock1.GetData buffer, , bytesTotal
    Text1.Text = buffer
    DoEvents
    If Winsock2.State <> sckClosed Then
                                          Winsock2.Close
    Winsock2.RemotePort = CDbl(Text2.Text)
    Winsock2.RemoteHost = Text3.Text
    On Error GoTo errore
    Winsock2.Connect
    Exit Sub
errore:
    MsgBox Err.Description
    Command2_Click
End Sub
```



```
Private Sub Winsock1_Error(ByVal Number As Integer,
Description As String, ByVal Scode As Long, ByVal Source
As String, ByVal HelpFile As String, ByVal
HelpContext As Long, CancelDisplay As Boolean)
    'Si commenta da sola.......
    Winsock1.Close
    Winsock1.Listen
    Label1.Caption = "SCONNESSO"
End Sub

Private Sub Winsock1_SendComplete()
    'Terminata la trasmissione chiudi le connessioni
    On Error Resume Next
    Winsock1.Close
    Winsock1.Listen
    Label1.Caption = "SCONNESSO"
    Winsock2.Close
End Sub

Private Sub Winsock2_Connect()
    'Quando il server risponde invia la richiesta
    On Error GoTo error3
    Dim buffer3 As String
    buffer3 = Text1.Text
    DoEvents
    Winsock2.SendData (buffer3)
    Exit Sub
error3:
    MsgBox Err.Description
End Sub
```



```
Private Sub Winsock2_DataArrival(ByVal bytesTotal As
                                                   Long)
    'Il server ha risposto: dillo al browser
    On Error GoTo errore2
    Dim buffer2 As String
    Winsock2.GetData buffer2, , bytesTotal
    RichTextBox1.Text = RichTextBox1.Text + buffer2
    DoEvents
    Winsock1.SendData ""
    Winsock1.SendData RichTextBox1.Text
    Exit Sub
errore2:
    MsgBox Err.Description
    Command2_Click
End Sub

Private Sub Winsock2_Error(ByVal Number As Integer,
Description As String, ByVal Scode As Long, ByVal Source
As String, ByVal HelpFile As String, ByVal
 HelpContext As Long, CancelDisplay As Boolean)
    'Problemi? Chiudi il socket!
    Winsock2.Close
End Sub
```